ECM3704 Number Theory 2015–2016

Henri Johnston
H.Johnston@exeter.ac.uk

10th December 2015

Abstract

These notes are based on the lecture notes and handouts of Dr Robin Chapman who gave this course in 2013–2014. The lectures were originally typed up by Oliver Bond who sat in on the course that year. The notes have since been completely rewritten, but considerable thanks is clearly due to both Robin and Oliver. All errors are my own; please do email me if you find any.

1 Divisibility and primes

1.1 Divisibility

Definition 1.1. We recall the definitions of the following sets.

(i) $\mathbb{N}$ (the natural numbers) is defined to be $\{1, 2, 3, \ldots\}$ (note $0 \notin \mathbb{N}$).
(ii) $\mathbb{Z}$ (the integers) is defined to be $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.
(iii) $\mathbb{Q}$ (the rational numbers) is defined to be $\{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$.

Remark 1.2. $(\mathbb{Z}, +, \times)$ is a commutative ring with 1 and $(\mathbb{Q}, +, \times)$ is a field.

Definition 1.3. Given $a, b \in \mathbb{Z}$, we say that 'a divides b' or 'a is a divisor of b' or 'b is a multiple of a' or 'a is a factor of b' if and only if there exists $c \in \mathbb{Z}$ such that $b = ac$. (If $a \neq 0$ this means $\frac{b}{a} \in \mathbb{Z}$.) The notation '$a \mid b$' means '$a$ divides b'.

Proposition 1.4. *Let $a, b, c, n, x, y \in \mathbb{Z}$. Divisibility has the following properties:*

(i) *$a \mid a$ (reflexive property),*
(ii) *$a \mid b$ and $b \mid c$ implies $a \mid c$ (transitive property),*
(iii) *$a \mid b$ and $a \mid c$ implies $a \mid (xb \pm yc)$ (linearity property),*

(iv) $a \mid b$ *implies* $an \mid bn$ *(multiplication property),*
(v) $an \mid bn$ *and* $n \neq 0$ *implies* $a \mid b$ *(cancellation property),*
(vi) $1 \mid n$ *(*1 *divides every integer),*
(vii) $n \mid 0$ *(every integer divides* 0*),*
(viii) $0 \mid n$ *implies* $n = 0$ *(zero divides only zero),*
(ix) $a \mid b$ *and* $b \neq 0$ *implies* $|a| \leq |b|$ *(comparison property),*
(x) $a \mid b$ *and* $b \mid a$ *implies* $|a| = |b|$*, i.e.,* $a = \pm b$*.*

Proof. Checking the properties is straightforward. We check (iii) and leave the others as an exercise. Since $a \mid b$ and $a \mid c$ there exist $m, n \in \mathbb{Z}$ such that $b = an$ and $c = am$. For any $x, y \in \mathbb{Z}$ we have

$$xb \pm yc = xan \pm yam = a(xn \pm ym).$$

So we have found an integer $q = xn \pm ym$ such that $xb \pm yc = aq$. Thus $a \mid (xb \pm yc)$, as desired. □

1.2 The Division Algorithm

Well-Ordering Principle (WOP). *Every non-empty subset of* $\mathbb{N} \cup \{0\}$ *contains a least element.*

Theorem 1.5 (The Division Algorithm)**.** *Given* $a \in \mathbb{Z}$*,* $b \in \mathbb{N}$*, there exist unique integers* q *and* r *satisfying* $a = bq + r$ *and* $0 \leq r < b$*.*

Proof. We first establish the existence of such a pair of integers q and r. Define $S := \{a - xb \mid x \in \mathbb{Z} \text{ and } a - xb \geq 0\}$. Note that $S \neq \emptyset$ since:

- if $a \geq 0$, by choosing $m = 0$, we get $a - mb = a \geq 0$;
- if $a < 0$, by choosing $m = a$, we get $a - mb = a - ab = (-a)(b-1) \geq 0$ since $-a > 0$ and $b > 0$.

Hence S is a non-empty subset of $\mathbb{N} \cup \{0\}$ and so by the Well-Ordering Principle S contains a least element $r \geq 0$. Since $r \in S$ we have there exists $q \in \mathbb{Z}$ such that $a - qb = r$, so $a = qb + r$. It remains to show that $r < b$. Assume for a contradiction that $r \geq b$ and let $r_1 = r - b \geq 0$. Then

$$a = qb + r = qb + (r_1 + b) = (q + 1)b + r_1$$

and so $a - (q + 1)b = r_1 \in S$ and is smaller than r: a contradiction. Hence q and r satisfy the required properties.

We now show that the pair q, r is unique. Assume that there is another pair of integers q', r' such that $a = q'b + r'$ with $0 \leq r' < b$. Then from $a = qb + r = q'b + r'$ we have $(q - q')b = r' - r$. If $q = q'$ then we must have $r = r'$ and we are done. Suppose for a contradiction that $q \neq q'$. Then

$$b \leq |q - q'||b| = |r' - r|.$$

However, since $0 \leq r, r' < b$ we must have $|r' - r| < b$, which gives a contradiction. □

1.3 The Greatest Common Divisor

Theorem 1.6. *Let $a, b \in \mathbb{Z}$. Then there exists a unique $d \in \mathbb{N} \cup \{0\}$ and (non-unique) $x, y \in \mathbb{Z}$ such that*

(i) *$d \mid a$ and $d \mid b$,*

(ii) *if $e \in \mathbb{Z}$, $e \mid a$ and $e \mid b$ then $e \mid d$,*

(iii) *$d = ax + by$.*

Proof. If $a = b = 0$, then it is easy to check that we must have $d = 0$. So suppose that a and b are not both zero. Let

$$S = \{am + bn \mid m, n \in \mathbb{Z} \text{ and } am + bn > 0\}.$$

Now $a^2 + b^2 > 0$ so S is a non-empty subset of $\mathbb{N}$. Hence by the Well-Ordering Principle, S has a minimal element $d > 0$ and we can write $d = ax + by$ for some $x, y \in \mathbb{Z}$.

By the Division Algorithm, $a = qd + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < d$. Suppose for a contradiction that $r \neq 0$. Then

$$0 < r = a - qd = a - q(ax + by) = (1 - qx)a - qby.$$

Hence $r \in S$. But $r < d$, contradicting the minimality of d in S. So we must have $r = 0$, i.e., $d \mid a$. The same argument also shows that $d \mid b$.

Suppose $e \in \mathbb{Z}$, $e \mid a$ and $e \mid b$. Then e divides any linear combination of a and b, so in particular, $e \mid d$.

Suppose that $e \in \mathbb{N} \cup \{0\}$ also satisfies (i) & (ii). Then $e \mid d$ and $d \mid e$ and so $d = \pm e$. But $d, e \geq 0$ so we have $d = e$. Thus d is unique. □

Corollary 1.7. *If $a, b \in \mathbb{Z}$ then there exists a unique $d \in \mathbb{N} \cup \{0\}$ such that*

(i) *$d \mid a$ and $d \mid b$,*

(ii) *if $e \in \mathbb{Z}$, $e \mid a$ and $e \mid b$ then $e \mid d$.*

Proof. The existence of such a d is given by Theorem 1.6. In the proof of uniqueness in Theorem 1.6, we only used properties (i) & (ii). □

Definition 1.8. Let $a, b \in \mathbb{Z}$. Then the d of Corollary 1.7 is called the greatest common divisor of a and b and is written $\gcd(a, b)$. (Note this is the same d as in Theorem 1.6.) This is sometimes also referred to as the highest common factor and written as $\text{hcf}(a, b)$. If $\gcd(a, b) = 1$ then a and b are said to be coprime or relatively prime.

Combining Theorem 1.6, Corollary 1.7 and Definition 1.8, we have:

Bezout's Identity. *Given $a, b \in \mathbb{Z}$ there exist (non-unique) $x, y \in \mathbb{Z}$ such that* $\gcd(a, b) = ax + by$.

Proposition 1.9. *Let $a, b, c \in \mathbb{Z}$. The gcd has the following properties:*
(i) $\gcd(a, b) = \gcd(b, a)$ *(commutative law),*
(ii) $\gcd(a, \gcd(b, c)) = \gcd(\gcd(a, b), c)$ *(associative law),*
(iii) $\gcd(ac, bc) = |c| \gcd(a, b)$ *(distributive law),*
(iv) $\gcd(a, 1) = \gcd(1, a) = 1$,
(v) $\gcd(a, 0) = \gcd(0, a) = |a|$,
(vi) $c \mid \gcd(a, b)$ *if and only if* $c \mid a$ *and* $c \mid b$,
(vii) $\gcd(a + cb, b) = \gcd(a, b)$.

Proof. Checking properties (i),(ii),(iv),(v) & (vi) is straightforward and is left as an exercise. (For property (vi) use Bezout's Identity and the linearity property of divisibility).

We prove (iii). Let $d = \gcd(a, b)$ and let $e = \gcd(ac, bc)$. We wish to show that $e = |c|d$. By property (vi), $cd \mid e = \gcd(ac, bc)$ since $cd \mid ac$ and $cd \mid bc$. By Bezout's Identity, there exist $x, y \in \mathbb{Z}$ such that $d = ax + by$. Then

$$cd = acx + bcy.$$

But $e \mid ac$ and $e \mid bc$ and so by linearity of divisibility we have $e \mid cd$. Therefore $|e| = |cd|$, i.e., $e = |c|d$.

Finally, we prove (vii). Let $e = \gcd(a + bc, b)$ and $f = \gcd(a, b)$. Then $e \mid (a + bc)$ and $e \mid b$. Thus by linearity of divisibility $e \mid a$. Hence $e \mid a$ and $e \mid b$ so by property (vi), we have $e \mid f$. Similarly, $f \mid a$ and $f \mid b$ so again by linearity of divisibility $f \mid (a + bc)$. Thus $f \mid (a + bc)$ and $f \mid b$ and so again by property (vi), we have $f \mid e$. Therefore $e \mid f$ and $f \mid e$ and $f, e \geq 0$ so we conclude that $e = f$. □

Remark 1.10. Note that $\gcd(a, b) = 0$ if and only if $a = b = 0$. Otherwise $\gcd(a, b) \geq 1$.

Theorem 1.11 (Euclid's Lemma). *Let $a, b, c \in \mathbb{Z}$. If $a \mid bc$ and* $\gcd(a, b) = 1$ *then $a \mid c$.*

Proof. Suppose that $a \mid bc$ and $\gcd(a, b) = 1$. By Bezout's Identity there exist $x, y \in \mathbb{Z}$ such that $1 = ax + by$. Hence $c = acx + bcy$. But $a \mid acx$ and $a \mid bcy$, so $a \mid c$ by the linearity property of divisibility. □

Theorem 1.12 (Solubility of linear equations in the integers). *Let $a, b, c \in \mathbb{Z}$. The equation*

$$ax + by = c$$

is soluble with $x, y \in \mathbb{Z}$ if and only if $\gcd(a, b) \mid c$.

Proof. Let $d = \gcd(a, b)$. Then $d \mid a$ and $d \mid b$ so if there exist $x, y \in \mathbb{Z}$ such that $c = ax + by$ then $d \mid c$ by linearity of divisibility. Now suppose that $d \mid c$. Then we can write $c = qd$ for some $q \in \mathbb{Z}$. By Bezout's Identity there exist $x', y' \in \mathbb{Z}$ such that $d = ax' + by'$. Hence $c = qd = aqx' + bqy'$ and so $x = qx'$ and $y = qy'$ gives a suitable solution. □

1.4 Euclid's Algorithm

Theorem 1.13 (Euclid's Algorithm)**.** *Let $a, b \in \mathbb{N}$ with $a \geq b > 0$ and $b \nmid a$. Let $r_0 = a$, $r_1 = b$ and apply the Division Algorithm repeatedly to obtain a set of remainders $r_2, r_3, \ldots, r_n, r_{n+1}$ defined successively by the relations*

$$\begin{array}{rcll} r_0 & = & r_1 q_1 + r_2, & 0 < r_2 < r_1, \\ r_1 & = & r_2 q_2 + r_3, & 0 < r_3 < r_2, \\ & \vdots & & \\ r_{n-2} & = & r_{n-1} q_{n-1} + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} & = & r_n q_n + r_{n+1}, & r_{n+1} = 0. \end{array}$$

Then the last non-zero remainder, r_n, is equal to $\gcd(a, b)$*.*

Proof. There is a stage at which $r_{n+1} = 0$ because the r_i are strictly decreasing and non-negative. Recall from Proposition 1.9 (vii) that for any $x, y, z \in \mathbb{Z}$ we have $\gcd(x, y) = \gcd(x + zy, y)$. In particular, we have

$$\gcd(r_i, r_{i+1}) = \gcd(r_{i+1} q_{i+1} + r_{i+2}, r_{i+1}) = \gcd(r_{i+2}, r_{i+1}) = \gcd(r_{i+1}, r_{i+2}).$$

Applying this result repeatedly gives

$$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \cdots = \gcd(r_{n-1}, r_n) = r_n$$

where the last equality is because $r_n \mid r_{n-1}$. □

Remark 1.14. One can also use Euclid's Algorithm to find $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$ by 'working backwards'.

Example 1.15. Work out the greatest common divisor of 841 and 160 and express it as a linear combination of 841 and 160:

$$\begin{array}{rcl} 841 & = & 160 \times 5 + 41 \\ 160 & = & 41 \times 3 + 37 \\ 41 & = & 37 \times 1 + 4 \\ 37 & = & 4 \times 9 + 1 \\ 4 & = & 1 \times 4 + 0. \end{array}$$

Hence $\gcd(841, 160) = 1$ (i.e. they are coprime) and working backwards gives:

$$\begin{aligned}
1 &= 37 \times 1 - 4 \times 9 \\
&= 37 \times 1 - (41 - 37) \times 9 \\
&= 37 \times 10 - 41 \times 9 \\
&= (160 - 3 \times 41) \times 10 - 41 \times 9 \\
&= 160 \times 10 - 41 \times 39 \\
&= 160 \times 10 - (841 - 160 \times 5) \times 39 \\
&= -39 \times 841 + 205 \times 160.
\end{aligned}$$

Note that such a solution is not unique. For example, we will also have

$$1 = (160 - 39) \times 841 + (205 - 841) \times 160 = 121 \times 841 - 636 \times 160.$$

1.5 The Extended Euclidean Algorithm

Instead of performing Euclid's Algorithm to compute $\gcd(a, b)$ and then 'working backwards' to compute $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$, one can instead compute x, y during the course of performing Euclid's Algorithm. This is known as the Extended Euclidean Algorithm.

The sequences of quotients q_i and remainders r_i are defined as in Theorem 1.13. We also define sequences of integers x_i, y_i such that $r_i = ax_i + by_i$. Recall that we defined r_n to be the last non-zero remainder and that $r_n = \gcd(a, b)$. Therefore we have $\gcd(a, b) = r_n = ax_n + by_n$ and so we set $(x, y) := (x_n, y_n)$.

So how do we explicitly find x_i and y_i? Recall that $r_0 = a$ and $r_1 = b$. Thus $r_0 = 1 \times a + 0 \times b$ and $r_1 = 0 \times a + 1 \times b$, and so we set $(x_0, y_0) := (1, 0)$ and $(x_1, y_1) := (0, 1)$. Now assume that $i \geq 2$ and that x_j, y_j are known for $j < i$. Then $r_{i-2} = r_{i-1}q_{i-1} + r_i$ and so we have

$$\begin{aligned}
r_i = r_{i-2} - r_{i-1}q_{i-1} &= (ax_{i-2} + by_{i-2}) - (ax_{i-1} + by_{i-1})q_{i-1} \\
&= a(x_{i-2} - x_{i-1}q_{i-1}) + b(y_{i-2} - y_{i-1}q_{i-1}).
\end{aligned}$$

Thus we set $x_i := x_{i-2} - x_{i-1}q_{i-1}$ and $y_i := y_{i-2} - y_{i-1}q_{i-1}$. In other words, for $i \geq 2$ we define (x_i, y_i) recursively by

$$(x_i, y_i) := (x_{i-2}, y_{i-2}) - q_{i-1}(x_{i-1}, y_{i-1}).$$

Example 1.16. We compute $\gcd(841, 160)$ and express it as a linear combination of 841 and 160 using the Extended Euclidean Algorithm.

i	r_{i-2}		r_{i-1}		q_{i-1}		r_i	x_i	y_i
0							841	1	0
1							160	0	1
2	841	$=$	160	$\times$	5	$+$	41	1	-5
3	160	$=$	41	$\times$	3	$+$	37	-3	16
4	41	$=$	37	$\times$	1	$+$	4	4	-21
5	37	$=$	4	$\times$	9	$+$	1	-39	205
6	4	$=$	1	$\times$	4	$+$	0		

Therefore $\gcd(841, 160) = 1 = 841 \times (-39) + 160 \times 205$.

1.6 Primes

Definition 1.17. Prime and composite numbers in $\mathbb{N}$:

(i) A number $p \in \mathbb{N}$ with $p > 1$ is prime if and only if its only divisors are 1 and p (i.e. if $n \in \mathbb{N}$ and $n \mid p$ then $n = 1$ or $n = p$).

(ii) A number $n \in \mathbb{N}$ with $n > 1$ is composite if and only if it is not prime (i.e. $n = ab$ for some $a, b \in \mathbb{N}$ with $a, b > 1$).

Note that $n = 1$ is neither prime nor composite.

Proposition 1.18. *If $n \in \mathbb{N}$ with $n > 1$ then n has a prime factor.*

Proof. We use strong induction, i.e., we prove that if for all $m \in \mathbb{N}$ with $1 < m < n$, m has a prime factor, then n has a prime factor.

Case (i): if n is prime, then n is a prime factor of n.

Case (ii): If n is composite then $n = ab$ where $a, b \in \mathbb{N}$ with $a, b > 1$. So $1 < a < n$. By the induction hypothesis, there is a prime p with $p \mid a$. Hence $p \mid a$ and $a \mid n$, so by the transitivity property of divisibility $p \mid n$. □

Proposition 1.19. *If $n \in \mathbb{N}$ with $n > 1$ then we can write $n = p_1 p_2 \cdots p_k$ where $k \in \mathbb{N}$ and $p_1, \ldots, p_k$ are (not necessarily distinct) primes.*

Proof. If n is prime then the result is clear. So suppose that n is composite. Then by Proposition 1.18 n has a prime factor, i.e., $n = p_1 n_1$ where p_1 is prime and $n_1 \in \mathbb{N}$ with $n_1 > 1$. If n_1 is prime, we are done. If n_1 is composite, it has a prime factor p_2 and we can write $n_1 = p_2 n_2$ where $n_2 \in \mathbb{N}$ with $n_2 > 1$. If n_2 is prime, we are done, otherwise we take out another prime factor and keep on going. The process does eventually terminate since $n > n_1 > n_2 > \cdots > 1$. Hence after at most n steps we obtain a prime factorisation of n. □

Example 1.20. We have $666 = 3 \times 222 = 3 \times 2 \times 111 = 3 \times 2 \times 3 \times 37$.

Theorem 1.21. *There are infinitely many primes.*

Euclid's proof. For a contradiction, assume $\{p_1, p_2, \ldots, p_n\}$ is a complete list of primes. Consider $N := 1 + p_1 p_2 \ldots p_n \in \mathbb{N}$. Then $N > 1$ so by Proposition 1.18, N has a prime factor p. However, every prime is supposedly one of $p_1, \ldots, p_n$, so $p = p_i$ for some i. Then $p = p_i \mid (p_1 \ldots p_n)$, so $p \mid (N - 1)$. However, we also have $p \mid N$ and we can write $1 = N - (N - 1)$, so $p \mid 1$, which is a contradiction. □

1.7 The Fundamental Theorem of Arithmetic

Lemma 1.22. *Let $n \in \mathbb{Z}$. If a prime p does not divide n then* $\gcd(p, n) = 1$.

Proof. Let $d = \gcd(p, n)$. Then $d \mid p$ so by definition of prime either $d = 1$ or $d = p$. But $d \mid n$ so $d \neq p$ because $p \nmid n$. Hence $d = 1$. □

Theorem 1.23 (Euclid's Lemma for Primes)**.** *Let $a, b \in \mathbb{Z}$ and let p a be prime. If $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Proof. Assume that $p \mid ab$ and that $p \nmid a$. We shall prove that $p \mid b$. By Lemma 1.22, $\gcd(p, a) = 1$ so by Euclid's Lemma (Theorem 1.11), $p \mid b$. □

Remark 1.24. Euclid's Lemma for Primes immediately generalises to several factors: if p is prime and $p \mid a_1 a_2 \ldots a_k$ then $p \mid a_j$ for some j.

Definition 1.25. Let $n \in \mathbb{N}$ and let p be a prime. Then

$$v_p(n) := \max\{k \in \mathbb{N} \cup \{0\} : p^k \mid n\}.$$

(Note that this set is always non-empty as it must contain 0; moreover, it is clear that it is bounded above.) In other words, k is the unique non-negative integer such that $p^k \mid n$ but $p^{k+1} \nmid n$. Equivalently, $v_p(n) = k$ if and only if $n = p^k n'$ where $n' \in \mathbb{N}$ and $p \nmid n'$. (For the right to left implication, use the cancellation property of divisibility.)

Example 1.26. The following example illustrates the definition of $v_p(n)$.

- $v_2(720) = 4$ because $\frac{720}{16} = 45$ is odd, so $2^4 \mid 720$ but $2^5 \nmid 720$.
- $v_3(720) = 2$ because $3 \nmid 80 = \frac{720}{9}$, so $3^2 \mid 720$ but $3^3 \nmid 720$.
- $v_5(720) = 1$ because $5 \nmid 144 = \frac{720}{5}$, so $5 \mid 720$ but $5^2 \nmid 720$.
- If $p \geq 7$ then $v_p(720) = 0$ because $p \nmid 720$.

Lemma 1.27. *Let $n, m \in \mathbb{N}$ and let p be a prime. Then*

$$v_p(mn) = v_p(m) + v_p(n).$$

Proof. Let $k = v_p(m)$ and $\ell = v_p(n)$. Then we can write $m = p^k m'$ where $p \nmid m'$ and similarly $n = p^\ell n'$ where $p \nmid n'$. Then $mn = p^{k+\ell} m'n'$. By Euclid's Lemma for Primes, $p \nmid m'n'$. Therefore $v_p(mn) = k + \ell$. □

Theorem 1.28 (The Fundamental Theorem of Arithmetic)**.** *Let $n \in \mathbb{N}$ with $n > 1$. Then*

(i) *(Existence) The number n can be written as a product of primes.*

(ii) *(Uniqueness) Suppose that*

$$n = p_1 \cdots p_r = q_1 \cdots q_s$$

where each p_i and q_j is prime. Assume further that

$$p_1 \le p_2 \le \cdots \le p_r \quad \text{and} \quad q_1 \le q_2 \le \cdots \le q_s.$$

Then $r = s$ and $p_i = q_i$ for all i.

Proof. The existence of a factorisation into primes is just Proposition 1.19.

Thus it remains to show uniqueness. Let ℓ be any prime. Then by Lemma 1.27 we have

$$v_\ell(n) = v_\ell(p_1 \cdots p_r) = v_\ell(p_1) + \cdots + v_\ell(p_r).$$

However,

$$v_\ell(p_i) = \begin{cases} 1 & \text{if } \ell = p_i, \\ 0 & \text{if } \ell \ne p_i. \end{cases}$$

Therefore

$$\begin{aligned} v_\ell(n) &= \#\text{ of } i \text{ for which } \ell = p_i \\ &= \#\text{ of times } \ell \text{ appears in the factorisation } n = p_1 \cdots p_r. \end{aligned}$$

Similarly,

$$v_\ell(n) = \#\text{ of times } \ell \text{ appears in the factorisation } n = q_1 \cdots q_s.$$

Thus every prime ℓ appears the same number of times in each factorisation, giving the desired result. □

Remark 1.29. Another way of interpreting this result is to say that for $n \in \mathbb{N}$

$$n = p_1^{v_{p_1}(n)} p_2^{v_{p_2}(n)} \cdots p_r^{v_{p_r}(n)}$$

where $p_1, \ldots, p_r$ are the distinct prime factors of n. Note that we take the empty product to be 1, which covers the case $n = 1$.

Lemma 1.30. *Let $n = \prod_{i=1}^r p_i^{a_i}$ where each $a_i \in \mathbb{N} \cup \{0\}$ and the p_i's are distinct primes. The set of positive divisors of n is the set of numbers of the form $\prod_{i=1}^r p_i^{c_i}$ where $0 \le c_i \le a_i$ for $i = 1, \ldots, r$.*

Proof. Exercise. □

2 Modular Arithmetic

2.1 Congruences

Definition 2.1. Suppose $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. We write $a \equiv b \bmod n$ (or $a \equiv b \pmod{n}$), and say 'a is congruent to b mod n', if and only if $n \mid (a-b)$. If $n \nmid (a-b)$ we write $a \not\equiv b \bmod n$ and say that 'a and b are incongruent mod n'.

Remark 2.2. In particular, $a \equiv 0 \bmod m$ if and only if $m \mid a$.

Examples 2.3. (i) $4 \equiv 30 \bmod 13$ since $13 \mid (4-30) = -26$.
(ii) $17 \not\equiv -17 \bmod 4$ since $17 - (-17) = 34$ but $4 \nmid 34$.
(iii) n is even if and only if $n \equiv 0 \bmod 2$.
(iv) n is odd if and only if $n \equiv 1 \bmod 2$.
(v) $a \equiv b \bmod 1$ for every $a, b \in \mathbb{Z}$.

Proposition 2.4. *Let $n \in \mathbb{N}$. Being congruent* mod n *is an equivalence relation, i.e., the relation is:*
(i) *Reflexive: For all $a \in \mathbb{Z}$ we have $a \equiv a \bmod n$.*
(ii) *Symmetric: Let $a, b \in \mathbb{Z}$. If $a \equiv b \bmod n$ then $b \equiv a \bmod n$.*
(iii) *Transitive: Let $a, b, c \in \mathbb{Z}$. If $a \equiv b \bmod n$ and $b \equiv c \bmod n$ then $a \equiv c \bmod n$.*

Proof. The proof follows at once from the following properties of divisibility:
(i) $n \mid 0$.
(ii) If $n \mid (a-b)$ then $n \mid (b-a)$.
(iii) If $n \mid (a-b)$ and $n \mid (b-c)$ then $n \mid (a-b)+(b-c) = (a-c)$. □

Proposition 2.5. *Congruences respect addition, subtraction and multiplication. Let $n \in \mathbb{N}$ and let $a, b, \alpha, \beta \in \mathbb{Z}$. Suppose that $a \equiv \alpha \bmod n$ and $b \equiv \beta \bmod n$. Then*
(i) *$a + b \equiv \alpha + \beta \bmod n$,*
(ii) *$a - b \equiv \alpha - \beta \bmod n$, and*
(iii) *$ab \equiv \alpha\beta \bmod n$.*
Moreover, if $f(x) \in \mathbb{Z}[x]$ then $f(a) \equiv f(\alpha) \bmod n$.

Proof. We will check that $ab \equiv \alpha\beta \bmod n$; the rest is an exercise. Since $a \equiv \alpha \bmod n$, we have $n \mid (a-\alpha)$ and so $a = \alpha + ns$ for some $s \in \mathbb{Z}$. Similarly, $b = \beta + nt$ for some $t \in \mathbb{Z}$. Hence

$$ab = (\alpha + ns)(\beta + nt) = \alpha\beta + n(s\beta + t\alpha + nst)$$

and so $n \mid (ab - \alpha\beta)$. Therefore $ab \equiv \alpha\beta \bmod n$, as required. □

Example 2.6. Let $n \in \mathbb{N}$ and write n in decimal notation

$$n = \sum_{i=0}^{k} a_i \times 10^i \text{ where } 0 \leq a_i \leq 9 \text{ and } a_i \in \mathbb{N} \cup \{0\} \text{ for all } i.$$

Define $f(x)$ by

$$f(x) = \sum_{i=0}^{k} a_i x^i.$$

Then, since $10 \equiv -1 \bmod 11$, we see that $n = f(10) \equiv f(-1) \bmod 11$, whence $11 \mid n \iff 11 \mid f(-1) \iff 11 \mid (a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^k a_k)$. This gives an easy way to test integers for divisibility by 11.

Example 2.7. Does the equation $x^2 - 3y^2 = 2$ have a solution with $x, y \in \mathbb{Z}$? Let $x, y \in \mathbb{Z}$. Note that $x^2 - 3y^2 \equiv x^2 \bmod 3$. Now $x \equiv 0, 1$ or $2 \bmod 3$, so $x^2 \equiv 0, 1$ or $4 \bmod 3$. But $4 \equiv 1 \bmod 3$ so in fact $x^2 \equiv 0$ or $1 \bmod 3$. Hence $x^2 - 3y^2 \equiv x^2 \not\equiv 2 \bmod 3$ and so $x^2 - 3y^2 \neq 2$.

Theorem 2.8. *There are infinitely many primes p with $p \equiv 3 \bmod 4$.*

Proof. If p is a prime then $p \equiv 0, 1, 2$ or $3 \bmod 4$. But $p \not\equiv 0 \bmod 4$ because $4 \nmid p$. If $p \equiv 2 \bmod 4$ then $p = 4k + 2$ for some $k \in \mathbb{Z}$ so $2 \mid p$ and so in fact $p = 2$. Therefore there are three types of primes:

(i) $p = 2$,
(ii) $p \equiv 1 \bmod 4$,
(iii) $p \equiv 3 \bmod 4$.

Let $N \in \mathbb{N}$. It suffices to show that there exists a type (iii) prime with $p > N$. Let $M = 4(N!) - 1$. Then $M \geq 3$ and so by the existence statement of Fundamental Theorem of Arithmetic (i.e. Proposition 1.19) M has a prime factorisation $M = p_1 p_2 \cdots p_k$. If p is a prime such that $p \leq N$ then $M \equiv -1 \bmod p$ so $p \nmid M$. Hence $p_j > N$ for all j. Moreover, $p_j \neq 2$ for all j because M is odd. Therefore for each j we have $p_j \equiv 1$ or $3 \bmod 4$. If $p_j \equiv 3 \bmod 4$ for any j then we are done. If this is not the case then $p_j \equiv 1 \bmod 4$ for all j, and so $M \equiv 1 \times \cdots \times 1 \equiv 1 \bmod 4$; but by definition of M we have $M \equiv -1 \equiv 3 \bmod 4$ - contradiction! □

Remark 2.9. Congruences do not respect division. For example, $4 \equiv 14 \bmod 10$ but $2 \not\equiv 7 \bmod 10$.

Proposition 2.10. *Let $a, b, s \in \mathbb{Z}$ and $d, n \in \mathbb{N}$.*

(i) *If $a \equiv b \bmod n$ and $d \mid n$ then $a \equiv b \bmod d$.*
(ii) *Suppose $s \neq 0$. Then $a \equiv b \bmod n$ if and only if $as \equiv bs \bmod ns$.*

Proof. (i) follows from the transitivity property of divisibility; (ii) follows from the multiplication and cancellation properties. □

Theorem 2.11 (Cancellation Law for Congruences)**.** *Let $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}$. Let $d = \gcd(c, n)$. Then $ac \equiv bc \bmod n \iff a \equiv b \bmod \frac{n}{d}$. In particular, if n and c are coprime, then $ac \equiv bc \bmod n \iff a \equiv b \bmod n$.*

Proof. Since $d = \gcd(c, n)$, we may write $n = dn'$ and $c = dc'$ where $n', c' \in \mathbb{Z}$.

Suppose $ac \equiv bc \bmod n$. Then $n \mid c(a - b)$ and hence the cancellation property of divisibility gives $n' \mid c'(a - b)$. However, $\gcd(n', c') = 1$ and so $n' \mid (a - b)$ by Euclid's Lemma. Thus $a \equiv b \bmod n'$.

Suppose conversely that $a \equiv b \bmod n'$. Then $n' \mid (a-b)$ and so $n \mid d(a-b)$. But $d \mid c$ so $d(a-b) \mid c(a-b)$ and thus $n \mid c(a-b)$ by the transitive property of divisibility. Thus $ac \equiv bc \bmod n$. □

Proposition 2.12. *Let $a, m, n \in \mathbb{Z}$. If m and n are coprime and if $m \mid a$ and $n \mid a$ then $mn \mid a$.*

Proof. Since $m \mid a$ we can write $a = mc$ for some $c \in \mathbb{Z}$. Now $n \mid a = mc$ and $\gcd(m, n) = 1$ so by Euclid's Lemma, $n \mid c$. Thus by the multiplicative property of divisibility, $mn \mid mc = a$. □

Corollary 2.13. *Let $m, n \in \mathbb{N}$ be coprime and let $a, b \in \mathbb{Z}$. If $a \equiv b \bmod m$ and $a \equiv b \bmod n$ then $a \equiv b \bmod mn$.*

Proof. We have $n \mid (a - b)$ and $m \mid (a - b)$. Since m and n are coprime we therefore have $mn \mid (a - b)$ by Proposition 2.12, i.e., $a \equiv b \bmod mn$. □

2.2 Residue classes and complete residue systems

Proposition 2.14. *Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \bmod n$ and $|b - a| < n$ then $a = b$.*

Proof. Since $n \mid (a - b)$, by the comparison property of divisibility we have $n \leq |a - b|$ unless $a - b = 0$. □

Recall Proposition 2.4 that congruence mod$n$ is an equivalence relation.

Definition 2.15. Consider a fixed modulus $n \in \mathbb{N}$. For $a \in \mathbb{Z}$ we write $[a]_n$ for the equivalence class of a mod n. Thus

$$[a]_n = \{x \in \mathbb{Z} \mid x \equiv a \bmod n\} = \{a + qn \mid q \in \mathbb{Z}\}.$$

This is called the residue class of a modulo n.

Example 2.16. Consider the case $n = 2$. Then

$$\begin{aligned}[0]_2 &= \{x \in \mathbb{Z} \mid x \equiv 0 \bmod 2\} = \{\text{the even integers}\},\\ [1]_2 &= \{x \in \mathbb{Z} \mid x \equiv 1 \bmod 2\} = \{\text{the odd integers}\}.\end{aligned}$$

To understand the results in this section, it is often helpful to think of the case $n = 2$ and odd and even integers.

Proposition 2.17. *Let $n \in \mathbb{N}$. The n residue classes $[0]_n, [1]_n, \dots, [n-1]_n$ are disjoint and their union is the set of all integers. In other words, every $x \in \mathbb{Z}$ is congruent modulo n to precisely one element of $\{0, 1, 2, \dots, n-1\}$.*

Proof. The integers $0, 1, 2, \dots, n-1$ are incongruent modulo n by Proposition 2.14. Hence the residue classes $[0]_n, [1]_n, \dots, [n-1]_n$ are distinct and thus disjoint (recall that distinct equivalences classes are always disjoint). Now every integer x must be in exactly one of these classes because by the Division Algorithm we can write $x = qn + r$ where $0 \le r < n$, so $x \equiv r \bmod n$ and hence $x \in [r]_n$. □

Definition 2.18. Let $n \in \mathbb{N}$. If S is a subset of $\mathbb{Z}$ containing exactly one element of each residue class modulo n we say that S is a complete residue system modulo n.

Remark 2.19. Proposition 2.17 says that $S = \{0, 1, 2, \dots, n-1\}$ is a complete residue system modulo n. Note that if S is any complete residue system modulo n we must have $|S| = n$ because Proposition 2.17 shows that there are precisely n residue classes modulo n. In fact, any set consisting of n integers, incongruent modulo n, is a complete residue system modulo n.

Examples 2.20. Let $n \in \mathbb{N}$. Then

$$\begin{gathered}\{0, 1, \dots, n-1\},\\ \{1, \dots, n\},\\ \{1, n+2, 2n+3, 3n+4, \dots, n^2\},\\ \{x \in \mathbb{Z} \mid -n/2 < x \le n/2\},\end{gathered}$$

are all complete residue systems modulo n.

Proposition 2.21. *Let $n \in \mathbb{N}$ and $k \in \mathbb{Z}$. Assume k and n are coprime. If $\{a_1, \dots, a_n\}$ is a complete residue system modulo n then so is $\{ka_1, \dots, ka_n\}$.*

Proof. If $ka_i \equiv ka_j \bmod n$ then by the cancellation law for congruences (Theorem 2.11) we have $a_i \equiv a_j \bmod n$ since $\gcd(k, n) = 1$. Therefore no two (distinct) elements in the set $\{ka_1, \dots, ka_n\}$ are congruent modulo n. Since there are n elements in this set, it forms a complete residue system. □

Example 2.22. The set $\{0, 1, 2, 3, 4\}$ is a complete residue system mod 5. Now $\gcd(2, 5) = 1$ so $\{2 \times 0, 2 \times 1, 2 \times 2, 2 \times 3, 2 \times 4\} = \{0, 2, 4, 6, 8\}$ is also a complete residue system mod 5.

2.3 Linear Congruences

The most basic congruences are *linear* congruences, i.e., those of the form

$$ax \equiv b \bmod n$$

to be solved for x. When the modulus n is small we can just use brute force, i.e., just try every possible value of x mod n. However, this quickly becomes impractical as n increases.

Theorem 2.23 (Linear congruences with exactly one solution)**.** *Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. Suppose that a and n are coprime. Then the linear congruence*

$$ax \equiv b \bmod n \tag{1}$$

has exactly one solution.

Proof. We need only test the numbers $1, 2, \ldots, n$ since they constitute a complete residue system. Therefore we consider the products $a, 2a, \ldots, na$. Since a and n are coprime, Proposition 2.21 shows that these numbers also constitute a complete system of residues modulo n. Hence exactly one of the elements of this set is congruent to b modulo n. In other words, there is exactly one x satisfying (1). □

Example 2.24. Let $a = 160, b = 3$ and $n = 841$. That is, we wish to solve

$$160x \equiv 3 \bmod 841. \tag{2}$$

Applying the Extended Euclidean Algorithm in this case shows that

$$\gcd(160, 841) = 1 = 160 \times 205 + 841 \times (-39). \tag{3}$$

(We did this calculation in Example 1.16.) Thus by Theorem 2.23 there is exactly one solution. Moreover, reducing equation (3) mod 841 gives

$$160 \times 205 \equiv 1 \bmod 841$$

and so multiplying through by 3 gives

$$160 \times (205 \times 3) \equiv 160 \times 615 \equiv 3 \bmod 841.$$

Therefore $x := 205 \times 3 = 615$ is the unique solution to (2) modulo 841.

Theorem 2.25 (Solubility of a linear congruence)**.** *Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. Then the linear congruence*

$$ax \equiv b \bmod n \tag{4}$$

has one or more solutions if and only if $\gcd(a, n) \mid b$.

Proof. By definition, the congruence (4) is soluble if and only if $n \mid (b - ax)$ for some $x \in \mathbb{Z}$, and this is true if and only if $b - ax = ny$ for some $x, y \in \mathbb{Z}$. Hence (4) is soluble if and only if

$$ax + ny = b$$

for some $x, y \in \mathbb{Z}$. Therefore the result now follows from Theorem 1.12 (solubility of linear equations in the integers). □

Theorem 2.26. *Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. Let $d = \gcd(a, n)$. Suppose that $d \mid b$ and write $a = da'$, $b = db'$ and $n = dn'$. Then the linear congruence*

$$ax \equiv b \bmod n \tag{5}$$

has exactly d solutions modulo n. These are given by

$$t, t + n', t + 2n', \ldots, t + (d - 1)n', \tag{6}$$

where t is the unique solution, modulo n', of the linear congruence

$$a'x \equiv b' \bmod n'. \tag{7}$$

Proof. Every solution of (5) is a solution of (7) and vice versa by Proposition 2.10. Since a' and n' are coprime, (7) has exactly one solution t modulo n' by Theorem 2.23. Thus the d numbers in (6) are solutions of (7) and hence of (5). No two of these are congruent modulo n since the relations

$$t + rn' \equiv t + sn' \bmod n \quad \text{with } 0 \leq r < d,\ 0 \leq s < d$$

imply

$$rn' \equiv sn' \bmod n, \quad \text{and hence } r \equiv s \bmod d,$$

where the last implication follows from Proposition 2.10 (note $n/n' = d$). But $0 \leq |r - s| < d$ so $r = s$ by Proposition 2.14.

It remains to show that (5) has no solutions other than those listed in (6). If y is a solution of (5) then $ay \equiv b \bmod n$. But we also have $at \equiv b \bmod n$ and so $ay \equiv at \bmod n$. Thus $y \equiv t \bmod n'$ by the cancellation law for congruences (Theorem 2.11). Hence $y = t + kn'$ for some $k \in \mathbb{Z}$. But

$r \equiv k \bmod d$ for some $r \in \mathbb{Z}$ such that $0 \leq r < d$. Therefore by Proposition 2.10 we have

$$kn' \equiv rn' \bmod n, \quad \text{and so } y \equiv t + rn' \bmod n.$$

Therefore y is congruent modulo n to one of the numbers in (6). □

Algorithm 2.27 (How to solve general linear congruences)**.** *Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. Suppose we wish to solve the linear congruence*

$$ax \equiv b \bmod n. \tag{8}$$

First apply the Extended Euclidean Algorithm to compute $d := \gcd(a, n)$ and find $x', y' \in \mathbb{Z}$ such that

$$ax' + ny' = d. \tag{9}$$

If $d \nmid b$ then there are no solutions by Theorem 2.25. Otherwise, there are exactly d solutions modulo n by Theorem 2.26, which we can find as follows.

Write $a = da'$, $b = db'$ and $n = dn'$. Dividing (9) through by d gives

$$a'x' + n'y' = 1.$$

Thus reducing mod n' gives $a'x' \equiv 1 \bmod n'$ and multiplying through by b' gives $a'(b'x') \equiv b' \bmod n'$. Therefore $t := b'x'$ is the unique solution to $a'x \equiv b' \bmod n'$ (the solution is unique because $\gcd(a', n') = 1$). Now by Theorem 2.26 the solutions to (8) are $t, t + n', t + 2n', \ldots, t + (d-1)n'$.

Example 2.28. Let $a = 33, b = 21$ and $n = 54$. That is, we wish to solve

$$33x \equiv 21 \bmod 54. \tag{10}$$

We apply the Extended Euclidean Algorithm as follows.

i	r_{i-2}		r_{i-1}		q_{i-1}		r_i	x_i	y_i
0							54	0	1
1							33	1	0
2	54	=	33	×	1	+	21	−1	1
3	33	=	21	×	1	+	12	2	−1
4	21	=	12	×	1	+	9	−3	2
5	12	=	9	×	1	+	3	5	−3
6	9	=	3	×	3	+	0		

Therefore

$$\gcd(54, 33) = 3 = ax_5 + ny_5 = 33 \times 5 + 54 \times (-3). \tag{11}$$

Thus there are exactly 3 solutions. Moreover, we have $a' = 11$, $b' = 7$ and $n' = 18$ and we may take $x' = 5$ and $y' = -3$. Hence

$$1 = a'x' + n'y' = 11 \times 5 + 18 \times (-3).$$

Reducing mod $n' = 18$ gives

$$11 \times 5 \equiv 1 \mod 18$$

and multiplying through by $b' = 7$ gives

$$11 \times (7 \times 5) \equiv 7 \mod 18.$$

Hence $t \equiv 7 \times 5 \equiv 35 \equiv 17 \bmod 18$ is the unique solution to

$$11x \equiv 7 \bmod 18.$$

Therefore the set of solutions to (10) modulo 54 is

$$\{17, 17 + (1 \times 18), 17 + (2 \times 18)\} = \{17, 35, 53\}.$$

2.4 The ring $\mathbb{Z}/n\mathbb{Z}$ and its units

Definition 2.29. Let $n \in \mathbb{N}$. We write $\mathbb{Z}/n\mathbb{Z} = \{[a]_n : 0 \leq a \leq n-1\}$ (so that $\#(\mathbb{Z}/n\mathbb{Z}) = n$). We set $[a]_n + [b]_n := [a+b]_n$ and $[a]_n[b]_n := [ab]_n$. (Note that Proposition 2.5 shows that these operations are well-defined).

Lemma 2.30. *The set $\mathbb{Z}/n\mathbb{Z}$, with the above operations, is a commutative ring with $0 = [0]_n$ and $1 = [1]_n$.*

Proof. Omitted and non-examinable. □

Definition 2.31. Let $n \in \mathbb{N}$. We write

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \in \mathbb{Z}/n\mathbb{Z} : \exists [b]_n \in \mathbb{Z}/n\mathbb{Z} \text{ such that } [a]_n[b]_n = [1]_n\}.$$

This is the set of units of $\mathbb{Z}/n\mathbb{Z}$, and is an abelian group under multiplication (check this!)

Proposition 2.32 (Units of $\mathbb{Z}/n\mathbb{Z}$)**.** *Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Then $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ if and only if $\gcd(a, n) = 1$.*

Proof. If $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ then the linear congruence $ax \equiv 1 \bmod n$ has a solution, and so by Theorem 2.25 (solubility of a linear congruence) we have $\gcd(a, n) \mid 1$. But $n > 0$ so in fact $\gcd(a, n) = 1$.

Suppose conversely that $\gcd(a, n) = 1$. Then by Theorem 2.23 (linear congruences with exactly one solution), the congruence $ax \equiv 1 \bmod n$ has exactly one solution, and so $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$. □

Definition 2.33. Let $n \in \mathbb{N}$ and let $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$. Then the unique solution to $ax \equiv 1 \bmod n$ is called the multiplicative inverse of a modulo n and is denoted $[a]_n^{-1} = [a^{-1}]_n$ or $a^{-1} \bmod n$.

Example 2.34. $\left(\frac{\mathbb{Z}}{12\mathbb{Z}}\right)^\times = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$.

2.5 Chinese Remainder Theorem

Theorem 2.35 (Chinese Remainder Theorem - a special case)**.** *Let $n, m \in \mathbb{N}$ be coprime and let $a, b \in \mathbb{Z}$ be given. Then the pair of linear congruences*

$$\begin{aligned} x &\equiv a \bmod m \\ x &\equiv b \bmod n \end{aligned}$$

has a solution $x \in \mathbb{Z}$. Moreover, if x' is any other solution then we have $x' \equiv x \bmod mn$.

Proof. Since n and m are coprime there exist $a', b' \in \mathbb{Z}$ such that $a'n \equiv 1 \bmod m$ and $b'm \equiv 1 \bmod n$ (use Theorem 2.23 or Theorem 2.25). Define $x := aa'n + bb'm$. Then $x \equiv aa'n \equiv a \bmod m$ and $x \equiv bb'm \equiv b \bmod n$. Hence x is a solution to the given pair of linear congruences.

Suppose $x' \equiv a \bmod m$ and $x' \equiv b \bmod n$. Then $m \mid (x - x')$ and $n \mid (x - x')$. Since m and n are coprime, it now follows from Proposition 2.12 that $mn \mid (x' - x)$. Hence $x \equiv x' \bmod nm$. □

Remark 2.36. We have used that m and n are coprime twice in the above proof. This hypothesis is necessary because, for example, the pair of congruences $x \equiv 2 \bmod 12$, $x \equiv 4 \bmod 20$ has no solution.

Example 2.37. Solve the following system of congruences:

$$\begin{aligned} x &\equiv 2 \bmod 3, \\ x &\equiv 3 \bmod 7. \end{aligned}$$

Note that 3 and 7 are indeed coprime because they are distinct primes. Following the proof, we set $a = 2$, $m = 3$, $b = 3$, $n = 7$. We have $mn = 3 \times 7 = 21$ and

$$\begin{aligned} 7a' &\equiv 1 \bmod 3 \implies \text{take } a' = 1, \\ 3b' &\equiv 1 \bmod 7 \implies \text{take } b' = 5. \end{aligned}$$

(Note that in more complicated situations we can use the Extended Euclidean Algorithm to compute multiplicative inverses modulo m and n.) Therefore

$$x = aa'n + bb'm = (2 \times 1 \times 7) + (3 \times 5 \times 3) = 14 + 45 = 59,$$

and the smallest positive integer solution is $17 \equiv 59 \bmod 21$.

Theorem 2.38 (Chinese Remainder Theorem). *Let $n_1, n_2, \dots, n_t \in \mathbb{N}$ with $\gcd(n_i, n_j) = 1$ whenever $i \neq j$, (i.e. the n_i are "coprime in pairs") and let $a_1, a_2, \dots, a_t \in \mathbb{Z}$ be given. Then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ &\vdots \\ x &\equiv a_t \bmod n_t \end{aligned}$$

has a solution $x \in \mathbb{Z}$. Moreover, if x' is any other solution, then $x' \equiv x \bmod N$, where $N := n_1 \cdots n_t$.

Proof. Define $N_i := N/n_i$. Then $\gcd(N_i, n_i) = 1$, since n_i is coprime to all the factors of N_i. Hence by Theorem 2.23 (or by Theorem 2.25) there exists $x_i \in \mathbb{Z}$ such that $N_i x_i \equiv 1 \bmod n_i$. Define $x := \sum_{i=1}^{t} a_i N_i x_i$. Thus $x \equiv a_k N_k x_k \bmod n_k$ since $n_k \mid N_i$ for all $i \neq k$. Therefore $x \equiv a_k(N_k x_k) \equiv a_k \bmod n_k$ for all k.

Suppose $x' \equiv a_k \bmod n_k$ for all k. Then $x' \equiv x \bmod n_k$ for all k. Thus $n_k \mid (x' - x)$ for all k. Since the n_i are pairwise coprime it now follows from Proposition 2.12 that $N := n_1 n_2 \cdots n_t \mid (x' - x)$. This yields $x' \equiv x \bmod N$. □

Example 2.39. Solve the following system of congruences:

$$\begin{aligned} x &\equiv 2 \bmod 3, \\ x &\equiv 3 \bmod 5, \\ x &\equiv 2 \bmod 7. \end{aligned}$$

Note that the $3, 5$ & 7 are indeed coprime in pairs because they are distinct primes. Following the proof, we put $N := 3 \times 5 \times 7 = 105$, $N_1 = 35$, $N_2 = 21$, $N_3 = 15$ and we have

$$\begin{aligned} 35x_1 &\equiv 1 \bmod 3 \implies \text{take } x_1 = 2, \\ 21x_2 &\equiv 1 \bmod 5 \implies \text{take } x_2 = 1, \\ 15x_3 &\equiv 1 \bmod 7 \implies \text{take } x_3 = 1. \end{aligned}$$

(Note that in more complicated situations we can use the Extended Euclidean Algorithm to compute multiplicative inverses modulo n.) Therefore

$$x = 2N_1x_1 + 3N_2x_2 + 2N_3x_3 = (2 \times 35 \times 2) + (3 \times 21 \times 1) + (2 \times 15 \times 1) = 233,$$

and the smallest positive integer solution is $23 \equiv 233 \bmod 105$.

2.6 Euler φ-function

Definition 2.40. For $n \in \mathbb{N}$, we define Euler's totient function, or the φ-function, by

$$\varphi(n) := \#\{a \in \mathbb{N} : 1 \leq a \leq n, \gcd(a,n) = 1\}.$$

Remark 2.41. $\varphi(1) = 1$ and for p prime, $\varphi(p) = \#\{1, 2, 3, \ldots, p-1\} = p-1$.

Remark 2.42. By Proposition 2.32 and the fact that $\{1, 2, \ldots, n\}$ is a complete residue system modulo n, we have that $\varphi(n) = \#\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$. Note that since $\gcd(0,n) = \gcd(n,n) = n$ for $n \in \mathbb{N}$, we also have

$$\varphi(n) = \#\{a \in \mathbb{Z} : 0 \leq a < n, \gcd(a,n) = 1\}.$$

Theorem 2.43. *Let $m, n \in \mathbb{N}$ be coprime. Then $\varphi(mn) = \varphi(m)\varphi(n)$.*

Proof. Let $a \in \mathbb{Z}$ with $0 \leq a < mn$ and define $b, c \in \mathbb{Z}$ by

$$a \equiv b \bmod m \quad \text{and} \quad a \equiv c \bmod n,$$

where $0 \leq b < m$ and $0 \leq c < n$. The Chinese Remainder Theorem tells us that there is a bijective correspondence between choices of a and choices of pairs (b,c). We now show that $\gcd(a, mn) = 1 \Leftrightarrow \gcd(b,m) = \gcd(c,n) = 1$. We shall use Proposition 2.32 (units of $\mathbb{Z}/n\mathbb{Z}$) several times.

Suppose $\gcd(a, mn) = 1$. Then the congruence $ax \equiv 1 \bmod mn$ has a solution $r \in \mathbb{Z}$, i.e, $ar \equiv 1 \bmod mn$. By Proposition 2.10 (i) we have $ar \equiv 1 \bmod m$ since $m \mid mn$. Hence $br \equiv ar \equiv 1 \bmod m$ and so the congruence $bx \equiv 1 \bmod m$ is soluble; thus $\gcd(b,m) = 1$. Similarly, $\gcd(c,n) = 1$.

Suppose conversely that $\gcd(b,m) = \gcd(c,n) = 1$. The congruences $bx \equiv 1 \bmod m$ and $cy \equiv 1 \bmod n$ are soluble so there exist $s, t \in \mathbb{Z}$ such that $bs \equiv 1 \bmod m$ and $ct \equiv 1 \bmod n$. Since m and n are coprime, by the Chinese Remainder Theorem there exists $r \in \mathbb{Z}$ such that $r \equiv s \bmod m$ and $r \equiv t \bmod n$. Hence $ar \equiv bs \equiv 1 \bmod m$ and $ar \equiv ct \equiv 1 \bmod n$ and so $x = ar$ is the solution to the simultaneous linear equations

$$x \equiv 1 \bmod m \quad \text{and} \quad x \equiv 1 \bmod n.$$

By the Chinese Remainder Theorem $ar \equiv 1 \bmod mn$. Hence $\gcd(a, mn) = 1$.

Therefore the number of integers a with $0 \leq a < mn$ which are coprime to mn, i.e. $\varphi(mn)$, is equal to the number of pairs of integers (b,c) with $0 \leq b < m$, $\gcd(b,m) = 1$ and $0 \leq c < n$, $\gcd(c,n) = 1$, i.e., $\varphi(m)\varphi(n)$. □

Theorem 2.44. *Let p be prime and let $r \in \mathbb{N}$. Then*

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1).$$

Proof. For all $m \in \mathbb{N}$, either $\gcd(p^r, m) = 1$ or $p \mid m$ (but not both). Thus

$$\begin{aligned}\varphi(p^r) &= \#\{m \in \mathbb{N} : m \leq p^r, p \nmid m\} \\ &= \#\{m \in \mathbb{N} : m \leq p^r\} - \#\{m \in \mathbb{N} : m \leq p^r, p \mid m\} \\ &= p^r - p^{r-1} = p^{r-1}(p-1). \qquad \square\end{aligned}$$

Examples 2.45. We can use these theorems to compute $\varphi(n)$ as follows:

- $\varphi(10) = \varphi(2 \times 5) = \varphi(2)\varphi(5) = (2-1)(5-1) = 1 \times 4 = 4$.
- $\varphi(12) = \varphi(2^2 \times 3) = \varphi(2^2)\varphi(3) = (2^2-2)(3-1) = 2 \times 2 = 4$.
- $\varphi(100) = \varphi(2^2 \times 5^2) = \varphi(2^2)\varphi(5^2) = (2^2-2)(5^2-5) = 2 \times 20 = 40$.
- $\varphi(1001) = \varphi(11 \times 91) = \varphi(11)\varphi(91) = 10\varphi(7 \times 13) = 10\varphi(7)\varphi(13) = 10 \times 6 \times 12 = 720$.

Proposition 2.46. *Let $n \in \mathbb{N}$. By the Fundamental Theorem of Arithmetic, we may write $n = p_1^{e_1} \cdots p_r^{e_r}$ where the p_i's are distinct primes and each $e_i \in \mathbb{N}$. Then*

$$\varphi(n) = \prod_{i=1}^{r} (p_i - 1)p^{e_i - 1}.$$

Proof. By Theorems 2.43 and 2.44 we have

$$\varphi(n) = \varphi(p_1^{e_1} \cdots p_r^{e_r}) = \prod_{i=1}^{r} \varphi(p_i^{e_i}) = \prod_{i=1}^{r} (p_i^{e_i} - p_i^{e_i - 1}) = \prod_{i=1}^{r} (p_i - 1)p_i^{e_i - 1}. \qquad \square$$

Corollary 2.47. *Let $n \in \mathbb{N}$. Then*

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

where the product runs over all distinct prime divisors of n.

Proof. From the above we have

$$\varphi(n) = \prod_{i=1}^{r} (p_i - 1)p_i^{e_i - 1} = \prod_{i=1}^{r} p_i^{e_i}(1 - p_i^{-1}) = n \prod_{i=1}^{r} (1 - p_i^{-1}) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

$\square$

Proposition 2.48. *For any $n \in \mathbb{N}$ we have $\sum_{d|n} \varphi(d) = n$.*

Proof. We classify the elements of $\{1, 2, \ldots, n\}$ according their greatest common divisor with n. Thus

$$\{a \in \mathbb{N} : a \leq n\} = \bigcup_{d|n} \{a \in \mathbb{N} : a \leq n, \, \gcd(n, a) = d\} \qquad \text{(disjoint union).}$$

Hence $n = \sum_{d|n} R_d$ where $R_d := \#\{a \in \mathbb{N} : 1 \leq 1a \leq n, \gcd(n, a) = d\}$. If $d \mid n$ then we can write $n = dn'$ with $n \in \mathbb{N}$ and by the distributive law for gcd's (Proposition 1.9 (iii)) we have $\gcd(n, a) = d$ if and only if $a = da'$ with $\gcd(n', a') = 1$. Moreover, $a \leq n$ if and only if $a' \leq n'$. It follows that

$$R_d = \#\{a' \in \mathbb{N} : 1 \leq a' \leq n', \gcd(n', a') = 1\},$$

and hence $R_d = \varphi(n')$. Therefore $n = \sum_{d|n} \varphi(\frac{n}{d})$. However, when $d \mid n$ we have $n = d \cdot \frac{n}{d}$; thus when d runs over the positive divisors of n, so does $e = \frac{n}{d}$, and therefore we have $n = \sum_{e|n} \varphi(e)$. □

Example 2.49. For $n = 12$ we have

$$\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12.$$

2.7 Exponentiation

Example 2.50. What is 3^k mod 19 as k varies?

k	0	1	2	3	4	5	6	7	8	9	10
3^k mod 19	1	3	9	8	5	15	7	2	6	18	16

k	11	12	13	14	15	16	17	18	19	20
3^k mod 19	10	11	14	4	12	17	13	1	3	9

Notice that the sequence repeats after a certain point. We can use the fact that $3^{18} \equiv 1 \bmod 19$ to simplify calculations. For example, by the Division Algorithm we have $100 = 5 \times 18 + 10$ so

$$3^{100} \equiv (3^{18})^5 3^{10} \equiv 1^5 3^{10} \equiv 3^{10} \equiv 16 \bmod 19.$$

Proposition 2.51. *Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. There exists $r \in \mathbb{N}$ such that $a^r \equiv 1 \bmod n$ if and only if $\gcd(a, n) = 1$.*

Proof. Suppose there exists $r \in \mathbb{N}$ such that $a^r \equiv 1 \bmod n$. Then a^{r-1} is a solution to $ax \equiv 1 \bmod n$ and so $\gcd(a, n) = 1$ by Proposition 2.32 (units of $\mathbb{Z}/n\mathbb{Z}$). Suppose conversely that $\gcd(a, n) = 1$. There are only finitely many possible values of $a^k \bmod n$ so there exist $i, j \in \mathbb{N}$ with $i < j$ such that $a^i \equiv a^j \bmod n$. Since $\gcd(a, n) = 1$ we may apply the cancellation law for congruences (Theorem 2.10) i times to obtain $a^{j-i} \equiv 1 \bmod n$. Thus we may take $r = j - i$. □

Definition 2.52. Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$ and suppose that $\gcd(a, n) = 1$. Then the least $d \in \mathbb{N}$ such that $a^d \equiv 1 \bmod n$ is called the order of $a \bmod n$, and written $\mathrm{ord}_n(a)$.

Proposition 2.53. *Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$ and suppose that* $\gcd(a, n) = 1$. *For $r, s \in \mathbb{Z}$ we have $a^r \equiv a^s \bmod n$ if and only if $r \equiv s \bmod \mathrm{ord}_n(a)$.*

Proof. Let $k = \mathrm{ord}_n(a)$. Then $a^k \equiv 1 \bmod n$. Assume without loss of generality that $r > s$. Suppose that $r \equiv s \bmod k$. Then there exists $t \in \mathbb{N}$ such that $r = s + tk$. Hence

$$a^r = a^s a^{kt} = a^s (a^k)^t \equiv a^s \bmod n.$$

Suppose conversely that $a^r \equiv a^s \bmod n$. Since $\gcd(a, n) = 1$ we may apply the cancellation law for congruences (Theorem 2.10) s times to obtain $a^{r-s} \equiv 1 \bmod n$. By the Division Algorithm, there exist $u, t \in \mathbb{N} \cup \{0\}$ such that $r - s = tk + u$ where $0 \leq u < k$. Then

$$a^{r-s} = a^{u+tk} = a^u (a^k)^t \equiv a^u 1^t \equiv a^u \bmod n$$

and so $a^u \equiv 1 \bmod n$. But $0 \leq u < k$ and k is the least *positive* integer such that $a^k \equiv 1 \bmod n$ and so we must have $u = 0$. Therefore $k \mid (r - s)$, i.e., $r \equiv s \bmod k$. □

Corollary 2.54. *Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$ and suppose that* $\gcd(a, n) = 1$. *Let $k \in \mathbb{Z}$. Then $a^k \equiv 1 \bmod n$ if and only if $\mathrm{ord}_n(a) \mid k$.*

Proof. Just take $r = k$ and $s = 0$ in Proposition 2.53. □

Corollary 2.55. *Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$ and suppose that* $\gcd(a, n) = 1$. *Then the numbers $1, a, a^2, \ldots, a^{\mathrm{ord}_n(a)-1}$ are incongruent mod n.*

Proof. Combine Propositions 2.14 and 2.53. □

2.8 Euler-Fermat Theorem

Definition 2.56. Let $n \in \mathbb{N}$. A subset R of $\mathbb{Z}$ is said to be a reduced residue system modulo n if
(i) R contains $\varphi(n)$ elements,
(ii) no two elements of R are congruent modulo n, and
(iii) for every $r \in R$ we have $\gcd(r, n) = 1$.

Remark 2.57. If R is a reduced residue system modulo n then

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n : a \in R\}.$$

Proposition 2.58. *Let $n \in \mathbb{N}$ and let $k \in \mathbb{Z}$. If $\{a_1, a_2, \dots, a_{\varphi(n)}\}$ is a reduced residue system modulo n and $\gcd(k, n) = 1$ then $\{ka_1, ka_2, \dots, ka_{\varphi(n)}\}$ is also a reduced residue system modulo n.*

Proof. If $ka_i \equiv ka_j \bmod n$ then by the cancellation law for congruences (Theorem 2.11) we have $a_i \equiv a_j \bmod n$ since $\gcd(k, n) = 1$. Therefore no two elements in the set $\{ka_1, \dots, ka_{\varphi(n)}\}$ are congruent modulo n. Moreover, since $\gcd(a_i, n) = \gcd(k, n) = 1$ we have $\gcd(ka_i, 1) = 1$ (check this!) so each ka_i is coprime to n. □

Theorem 2.59 (The Euler-Fermat Theorem)**.** *Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$ and suppose that $\gcd(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 \bmod n$.*

Proof. Let $\{b_1, b_2, \dots, b_{\varphi(n)}\}$ be a reduced residue system modulo n. Then since $\gcd(a, n) = 1$ the set $\{ab_1, ab_2, \dots, ab_{\varphi(n)}\}$ is also a reduced residue system by Proposition 2.58. Hence the product of all the integers in the first set is congruent modulo n to the product of those in the second set. Therefore

$$b_1 \cdots b_{\varphi(n)} \equiv a^{\varphi(m)} b_1 \cdots b_{\varphi(n)} \bmod n.$$

Since each b_i is coprime to n, we may apply the cancellation law for congruences (Theorem 2.11) $\varphi(n)$ times to obtain the desired result. □

Corollary 2.60. *Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$ and suppose that $\gcd(a, n) = 1$. Then $\mathrm{ord}_n(a) \mid \varphi(n)$.*

Proof. Combine the Euler-Fermat Theorem and Corollary 2.54. □

Example 2.61. We have $\varphi(12) = \varphi(2^2)\varphi(3) = 2 \times 2 = 4$. So for every $a \in \mathbb{Z}$ with $\gcd(a, 12) = 1$ we must have $\mathrm{ord}_{12}(a) = 1, 2$ or 4. In fact, $\mathrm{ord}_{12}(1) = 1$ and $\mathrm{ord}_{12}(5) = \mathrm{ord}_{12}(7) = \mathrm{ord}_{12}(11) = 2$, so working mod 12 there is no element element of order $\varphi(12) = 4$.

Corollary 2.62. *Let p be prime and let $a \in \mathbb{Z}$ such that $p \nmid a$. Then $a^{p-1} \equiv 1 \bmod p$.*

Proof. This follows immediately from the Euler-Fermat Theorem (Theorem 2.59) since $\varphi(p) = p - 1$. □

Example 2.63. We saw in Example 2.50 that $\mathrm{ord}_{19}(3) = 18 = \varphi(19)$. We also have $\mathrm{ord}_{19}(8) = 6$, which is a factor of 18.

Theorem 2.64 (Fermat's Little Theorem)**.** *Let p be prime and let $a \in \mathbb{Z}$. Then $a^p \equiv a \bmod p$.*

Proof. If $p \nmid a$ this follows easily from Corollary 2.62. If $p \mid a$ then both a^p and a are congruent to $0 \bmod p$. □

Remark 2.65. Sometimes the result of Corollary 2.62 is also referred to as Fermat's Little Theorem.

Remark 2.66. Many of the results in this section and the previous section can thought of in terms of group theory once we recall that $(\mathbb{Z}/n\mathbb{Z})^\times$ is an (abelian) group. For example, $\mathrm{ord}_n(a)$ is the order of $[a]_n$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. Moreover, Lagrange's Theorem in group theory tells us that the order of an element divides the order of the group; so $\mathrm{ord}_n(a)$ divides $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$ which gives the Euler-Fermat Theorem.

2.9 Binary powering algorithm

We briefly illustrate this algorithm with an example.

Example 2.67. Suppose that we want to compute $3^{499} \bmod 997$ efficiently. Note that 997 is prime so Fermat's Little Theorem tells us that $3^{996} \equiv 1 \bmod 997$. Unfortunately, this doesn't appear to help us. First we find the binary expansion of 499 as follows:

$$\begin{aligned}
499 &= 2^8 + 243 \\
&= 2^8 + 2^7 + 115 \\
&= 2^8 + 2^7 + 2^6 + 51 \\
&= 2^8 + 2^7 + 2^6 + 2^5 + 19 \\
&= 2^8 + 2^7 + 2^6 + 2^5 + 2^4 + 3 \\
&= 2^8 + 2^7 + 2^6 + 2^5 + 2^4 + 2^1 + 2^0.
\end{aligned}$$

So the binary expansion of 499 is 111110011. Now by squaring the previous term each time, we have

$$\begin{aligned}
3^{2^1} &\equiv 9 \pmod{997}\\
3^{2^2} &\equiv 9^2 \equiv 81 \pmod{997}\\
3^{2^3} &\equiv 81^2 \equiv 6561 \equiv 579 \equiv -418 \pmod{997}\\
3^{2^4} &\equiv (-418)^2 \equiv 418^2 \equiv 174724 \equiv 249 \pmod{997}\\
3^{2^5} &\equiv 249^2 \equiv 62001 \equiv 187 \pmod{997}\\
3^{2^6} &\equiv 187^2 \equiv 34969 \equiv 74 \pmod{997}\\
3^{2^7} &\equiv 74^2 \equiv 5476 \equiv 491 \pmod{997}\\
3^{2^8} &\equiv 491^2 \equiv 804 \equiv -193 \pmod{997}.
\end{aligned}$$

Therefore

$$\begin{aligned}
3^{499} &\equiv 3^{2^0} \times 3^{2^1} \times 3^{2^4} \times 3^{2^5} \times 3^{2^6} \times 3^{2^7} \times 3^{2^8} \pmod{997}\\
&\equiv 3 \times 9 \times 249 \times 187 \times 74 \times 491 \times (-193) \pmod{997}\\
&\equiv 27 \times 46563 \times 36334 \times (-193) \pmod{997}\\
&\equiv 27 \times 701 \times 442 \times (-193) \pmod{997}\\
&\equiv 18927 \times (-85306) \pmod{997}\\
&\equiv (-16) \times 436 \pmod{997}\\
&\equiv -6976 \pmod{997}\\
&\equiv 3 \pmod{997}.
\end{aligned}$$

Note that the advantage of this method is that it minimizes the number of multiplications we need to perform and that each integer we consider has at most twice the number of digits as the modulus.

2.10 Polynomial Congruences

Theorem 2.68 (Lagrange's polynomial congruence theorem)**.** *Let*

$$f(x) = a_0 + a_1 x + \cdots + a_d x^d \in \mathbb{Z}[x]$$

and let p *be a prime with* $p \nmid a_d$*. Then* $f(x) \equiv 0 \bmod p$ *has at most* d *solutions mod* p*.*

Remark 2.69. More generally, any polynomial equation of degree d over a field has at most d solutions (note that $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a field).

Proof. The proof is by induction on d. When $d = 1$ the congruence is linear:

$$a_1 x + a_0 \equiv 0 \bmod p.$$

Since $a_1 \not\equiv 0 \bmod p$ we have $\gcd(a_1, p) = 1$ and so there is exactly one solution by Theorem 2.23 (linear congruences with exactly one solution).

Assume that the theorem is true for polynomials of degree $d-1$. Suppose for a contradiction that the congruence $f(x) \equiv 0 \bmod p$ has $d+1$ incongruent solutions modulo p, say $x_0, x_1, x_2, \ldots, x_d$ where $f(x_k) \equiv 0 \bmod p$ for each $k = 0, 1, \ldots, d$. Recall that for any $r \in \mathbb{N}$ we have the algebraic identity

$$x^r - y^r = (x-y)(x^{r-1} + x^{r-2}y + x^{r-3}y^2 + \cdots + xy^{r-2} + y^{r-1}).$$

Thus we also have an algebraic identity

$$f(x) - f(x_0) = \sum_{r=1}^{d} a_r(x^r - x_0^r) = \sum_{i=1}^{d} a_r(x - x_0)g_r(x)$$

where each $g_r \in \mathbb{Z}[x]$ is of degree $r-1$ and has leading coefficient 1. Hence we have $f(x) - f(x_0) = (x - x_0)g(x)$ where $g(x) = \sum_{r=1}^{d} a_r g_r(x)$ is of degree $d-1$ and has leading coefficient a_d. Thus

$$f(x_k) - f(x_0) = (x_k - x_0)g(x_k) \equiv 0 \bmod p,$$

since $f(x_k) \equiv f(x_0) \equiv 0 \bmod p$. But $x_k - x_0 \not\equiv 0 \bmod p$ if $k \neq 0$ so we must have $g(x_k) \equiv 0 \bmod p$ for each $k \neq 0$ (we may apply the cancellation law for congruences (Theorem 2.11) because $\gcd(x - x_0, p) = 1$). But this means that the congruence $g(x) \equiv 0 \bmod p$ has d incongruent solutions modulo p, contradicting the induction hypothesis. □

Example 2.70. Note that $x^2 - 1 \equiv 0 \bmod 8$ has 4 roots, namely $1, 3, 5, 7 \bmod 8$. This is not a counterexample to Theorem 2.68, however, because 8 is not prime (and $\mathbb{Z}/8\mathbb{Z}$ is not a field).

Corollary 2.71. *Let $a \in \mathbb{Z}$ and let p be an odd prime. If $a^2 \equiv 1 \bmod p$ then $a \equiv \pm 1 \bmod p$.*

Proof. Lagrange's polynomial congruence theorem (Theorem 2.68) says that $a^2 \equiv 1 \bmod p$ has at most two solutions. But it is clear that $a \equiv \pm 1 \bmod p$ are solutions and these must be distinct because p is odd. Therefore, we have found all the solutions. □

Example 2.72. Let p and q be distinct odd primes. Consider the congruence

$$x^2 \equiv 1 \bmod pq.$$

It is clear that $x \equiv \pm 1 \bmod pq$ are solutions, but are there other solutions? By the Chinese Remainder Theorem we have

$$\begin{aligned} & x^2 \equiv 1 \bmod pq \\ & \quad \Longleftrightarrow \text{both } x^2 \equiv 1 \bmod p \text{ and } x^2 \equiv 1 \bmod q \\ & \quad \Longleftrightarrow \text{both } x \equiv \pm 1 \bmod p \text{ and } x \equiv \pm 1 \bmod q. \end{aligned}$$

Thus there are four solutions modulo pq. Note that

$$x \equiv 1 \bmod pq \Longleftrightarrow \begin{cases} x \equiv 1 \bmod p \\ x \equiv 1 \bmod q \end{cases}$$

and

$$x \equiv -1 \bmod pq \Longleftrightarrow \begin{cases} x \equiv -1 \bmod p \\ x \equiv -1 \bmod q \end{cases}$$

which are the "easy" solutions we already mentioned. It remains to solve the two pairs of congruences

$$\begin{cases} x \equiv 1 \bmod p \\ x \equiv -1 \bmod q \end{cases} \text{and} \begin{cases} x \equiv -1 \bmod p \\ x \equiv 1 \bmod q. \end{cases}$$

Note that we can use a trick here to save work: if x is the solution to one of these pairs of congruences then $-x$ is the solution to the other congruence.

Consider the following explicit example. We wish to find all solutions to

$$x^2 \equiv 1 \bmod 145.$$

Thus it is clear that $x \equiv \pm 1 \bmod 145$ gives two solutions, but we also want to find the other two solutions. Note that $145 = 5 \times 29$ and that both 5 and 29 are prime. Thus we want to solve

$$\begin{cases} x \equiv 1 \bmod 5 \\ x \equiv -1 \bmod 29. \end{cases}$$

By the Extended Euclidean Algorithm, we have

$$\gcd(5, 29) = 1 = 6 \times 5 - 1 \times 29$$

Thus using the construction of the Chinese Remainder Theorem we may take

$$x \equiv (-1) \times 6 \times 5 + 1 \times (-1) \times 29 \equiv -59 \bmod 145.$$

Check that this really is a solution:

$$(-59)^2 = 3481 = 1 + 24 \times 145 \equiv 1 \bmod 145.$$

Therefore the solutions of $x^2 \equiv 1 \bmod 145$ are $x \equiv \pm 1, \pm 59 \bmod 145$.

2.11 Hensel Lifting

The Chinese Remainder Theorem shows that the problem of solving a polynomial congruence

$$f(x) \equiv 0 \bmod n$$

can be reduced to solving a system of congruences

$$f(x) \equiv 0 \bmod p_i^{e_i} \quad (i = 1, \ldots, r)$$

where $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorisation of n. We show that this can be further reduced to congruences with prime moduli together with a set of linear congruences.

Theorem 2.73 (Hensel's Lemma)**.** *Let p be prime. Let $f(x) \in \mathbb{Z}[x]$ and let $f'(x) \in \mathbb{Z}[x]$ be its formal derivative. If $a \in \mathbb{Z}$ satisfies*

$$f(a) \equiv 0 \bmod p, \quad f'(a) \not\equiv 0 \bmod p$$

then for each $n \in \mathbb{N}$ there exists $a_n \in \mathbb{Z}$ such that

$$f(a_n) \equiv 0 \bmod p^n \quad \textit{and} \quad a_n \equiv a \bmod p. \tag{12}$$

Moreover, a_n is unique modulo p^n.

Example 2.74. Suppose we want to solve $x^2 \equiv -1 \bmod 5^4$. This is the same as solving the equation $f(x) \equiv 0 \bmod 5^4$ where $f(x) = x^2 + 1$. Note that $f'(x) = 2x$. An exhaustive search shows that $x = \pm 2$ are the solutions to $f(x) \equiv 0 \bmod 5$. Choose $a = 2$. Then $f(a) \equiv 0 \bmod 5$ and $f'(a) = 2 \times 2 = 4 \not\equiv 0 \bmod 5$. Thus we may apply Hensel's Lemma. Write $a_2 = 2 + 5t_1$. Then we have

$$\begin{aligned} f(2+5t_1) \equiv 0 \bmod 5^2 &\iff (2+5t_1)^2 + 1 \equiv 0 \bmod 5^2 \\ &\iff 4 + 20t_1 + 25t_1^2 + 1 \equiv 0 \bmod 5^2 \\ &\iff 5 + 20t_1 \equiv 0 \bmod 5^2 \\ &\iff 1 + 4t_1 \equiv 0 \bmod 5 \\ &\iff 4t_1 \equiv -1 \bmod 5 \\ &\iff t_1 \equiv 1 \bmod 5. \end{aligned}$$

Thus we may take $a_2 = 2+5\times1 = 7$. Check: $7^2 = 49 \equiv -1 \bmod 25$. We could now set $a_3 = 7+5^2t_2$ and find t_2 by solving the congruence $f(a_3) \equiv 0 \bmod 5^3$.

But instead we can take a short-cut as follows. Write $a_4 = 7 + 5^2 t_3$ and try to solve mod 5^4 directly. Then we have

$$\begin{aligned} f(7+5^2t_3) \equiv 0 \bmod 5^4 &\iff (7+5^2t_3)^2 + 1 \equiv 0 \bmod 5^4 \\ &\iff 49 + (14\times 25)t_3 + 5^4t_3^2 + 1 \equiv 0 \bmod 5^4 \\ &\iff 50 + (14\times 25)t_3 \equiv 0 \bmod 5^4 \\ &\iff 2 + 14t_3 \equiv 0 \bmod 5^2 \\ &\iff 1 + 7t_3 \equiv 0 \bmod 5^2 \\ &\iff 7t_3 \equiv -1 \bmod 5^2 \\ &\iff t_3 \equiv 7 \bmod 5^2. \end{aligned}$$

So we have $a_4 = 7 + 5^2 \times 7 = 182$. Check: $182^2 = 33,124 \equiv -1 \bmod 5^4$. Note that if we had started with the solution $a = -2$ then we would have ended up with the solution $a_4 = -182$.

Remark 2.75. Even if the hypotheses of Hensel's Lemma are not satisfied, we can still try to use the same technique to solve the given polynomial equation. However, in this case, the solutions are not guaranteed to exist or to be unique.

Lemma 2.76. *Let $f \in \mathbb{Z}[X]$ and let $f'(X)$ be its formal derivative. Then there exists $g \in \mathbb{Z}[X,Y]$ satisfying the polynomial identity*

$$f(X+Y) = f(X) + f'(X)Y + g(X,Y)Y^2.$$

Proof. This formula comes from isolating the first two terms in the binomial theorem. Writing $f(X) = \sum_{i=0}^{d} c_i X^i$ we have

$$f(X+Y) = \sum_{i=0}^{d} c_i(X+Y)^i = c_0 + \sum_{i=1}^{d} c_i(X^i + iX^{i-1}Y + g_i(X,Y)Y^2)$$

where $g_i(X,Y) \in \mathbb{Z}[X,Y]$. Thus

$$\begin{aligned} f(X+Y) &= \sum_{i=0}^{d} c_i X^i + \sum_{i=1}^{d} ic_i X^{i-1}Y + \sum_{i=1}^{d} c_i g_i(X,Y)Y^2 \\ &= f(X) + f'(X)Y + g(X,Y)Y^2 \end{aligned}$$

where $g(X,Y) := \sum_{i=1}^{d} c_i g_i(X,Y)$. This gives the desired identity. □

Remark 2.77. The identity of Lemma 2.76 is similar to Taylor's formula:

$$f(x+h) = f(x) + f'(x)h + (f''(x)/2!)h^2 + \cdots .$$

The problem is that the terms Taylor's formula have factorials in the denominator, which can cause problems when reducing modulo powers of p: think about $f''(x)/2! \bmod 2$, for example.

Proof of Hensel's Lemma. We will prove by induction that for each $n \in \mathbb{N}$ there exists a $a_n \in \mathbb{Z}$ satisfying (12) that is unique mod p^n. The case $n = 1$ is trivial using $a_1 = a$. We now suppose the inductive hypothesis holds for $n = k$ and show it holds for $n = k + 1$. The idea is to consider $a_k + p^k t_k$ and see if $t_k \in \mathbb{Z}$ can be chosen in such a way that $a_k + p^k t_k$ satisfies the required properties of a_{k+1}.

By Lemma 2.76 with $X = a_k$ and $Y = p^k t_k$ there exists $z_k \in \mathbb{Z}$ such that

$$f(a_k + p^k t_k) = f(a_k) + f'(a_k)p^k t_k + z_k p^{2k} t_k^2 \equiv f(a_k) + f'(a_k)p^k t_k \bmod p^{k+1}$$

where the congruence follows since $k + 1 \leq 2k$. In $f'(a_k)p^k t_k \bmod p^{k+1}$ the factors $f'(a_k)$ and t_k only matter mod p since it already contains a factor of p^k and the modulus is p^{k+1}. Thus recalling that $a_k \equiv a \bmod p$ we have $f'(a)p^k t_k \equiv f'(a_k)p^k t_k \bmod p^{k+1}$. Therefore we have

$$\begin{aligned} f(a_k + p^k t_k) \equiv 0 \bmod p^{k+1} &\iff f(a_k) + f'(a)p^k t_k \equiv 0 \bmod p^{k+1} \\ &\iff f'(a)t_k \equiv -f(a_k)/p^k \bmod p, \end{aligned} \tag{13}$$

where the ratio $-f(a_k)/p^k$ is in $\mathbb{Z}$ since we have $f(a_k) \equiv 0 \bmod p^k$ by the induction hypothesis, and the last equivalence follows from Proposition 2.10. But $f'(a) \not\equiv 0 \bmod p$ so $\gcd(f'(a), p) = 1$ and thus by Theorem 2.23 (linear congruences with exactly one solution) the last congruence (mod p) has a solution t_k, which is unique mod p.

We set $a_{k+1} = a_k + p^k t_k$. Then we have $f(a_{k+1}) \equiv 0 \bmod p^{k+1}$ and $a_{k+1} \equiv a_k \bmod p^k$, so in particular $a_{k+1} \equiv a \bmod p$. It remains to show uniqueness. Suppose there exists $b_{k+1} \in \mathbb{Z}$ with $f(b_{k+1}) \equiv 0 \bmod p^{k+1}$ and $b_{k+1} \equiv a \bmod p$. Then we also have $f(b_{k+1}) \equiv 0 \bmod p^k$ and so by the uniqueness of a_k we must have $b_{k+1} \equiv a_k \bmod p^k$. Thus $b_{k+1} = a_k + p^k s_k$ for some $s_k \in \mathbb{Z}$. But (13) and the proceeding discussion shows that $s_k \equiv t_k \bmod p$ and thus we must have $a_{k+1} \equiv b_{k+1} \bmod p^{k+1}$, as desired. □

Remark 2.78. An adaptation of the above proof shows that under the assumptions of Hensel's Lemma, in principle one can always lift from a solution mod p^k to a solution mod p^{2k}. Moreover, for $m \geq n \geq 1$ we always have $a_m \equiv a_n \bmod p^n$.

2.12 Primitive Roots

Recall Corollary 2.60: if $n \in \mathbb{N}$, $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$ then $\operatorname{ord}_n(a) \mid \varphi(n)$. In this section, we shall be interested in the case that $\operatorname{ord}_n(a) = \varphi(n)$.

Definition 2.79. Let $n \in \mathbb{N}$. We say that $a \in \mathbb{Z}$ is a primitive root mod n if and only if $\gcd(a, n) = 1$ and $\operatorname{ord}_n(a) = \varphi(n)$.

Remark 2.80. This is equivalent to requiring $[a]_n$ to be a generator for the abelian group $(\mathbb{Z}/n\mathbb{Z})^\times$, which must therefore be cyclic.

Example 2.81. Let $n = 5$ and abbreviate $[x]_n = [x]_5$ to $[x]$. Then we have

$$[2]^0 = [1], \quad [2]^1 = [2], \quad [2]^2 = [4], \quad [2]^3 = [8] = [3], \quad [2]^4 = [16] = [1].$$

Therefore $\operatorname{ord}_5(2) = 4 = \varphi(5)$ and so 2 is a primitive root of 5.

Remark 2.82. For some values of n there are no primitive roots. For example, every non-trivial element of $(\mathbb{Z}/8\mathbb{Z})^\times = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ has order 2, and so $(\mathbb{Z}/8\mathbb{Z})^\times$ is not cyclic. Example 2.61 shows that the same is true for $(\mathbb{Z}/12\mathbb{Z})^\times$.

Lemma 2.83. *Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Then for $k \in \mathbb{Z}$ we have*

$$\operatorname{ord}_n(a^k) = \frac{\operatorname{ord}_n(a)}{\gcd(\operatorname{ord}_n(a), k)}.$$

In particular, $\operatorname{ord}_n(a^k) = \operatorname{ord}_n(a)$ *if and only if* $\gcd(\operatorname{ord}_n(a), k) = 1$.

Proof. Let $f = \operatorname{ord}_n(a)$. The integer $\operatorname{ord}_n(a^k)$ is the least $d \in \mathbb{N}$ such that $a^{dk} \equiv 1 \bmod n$. By Corollary 2.54 this is also the least $d \in \mathbb{N}$ such that $dk \equiv 0 \bmod f$. But by the cancellation law for congruences (Theorem 2.11) this last congruence is equivalent to the congruence $d \equiv 0 \bmod \frac{f}{h}$ where $h = \gcd(f, k)$. But it is clear that the least positive solution to this congruence is $d = \frac{f}{h}$ and so $\operatorname{ord}_n(a^k) = \frac{f}{h}$, as asserted. □

Example 2.84. We saw in Example 2.50 that 3 is a primitive root mod 19, i.e., $\operatorname{ord}_{19}(3) = \varphi(19) = 18$. Thus $\operatorname{ord}_{19}(3^3) = \operatorname{ord}_{19}(8) = 18/\gcd(18, 3) = 18/3 = 6$.

Theorem 2.85. *Let p be prime and let $d \in \mathbb{N}$ be a divisor of $p - 1$. Then there are exactly $\varphi(d)$ elements $a \bmod p$ such that $\operatorname{ord}_p(a) = d$. In particular, there are $\varphi(p - 1)$ primitive roots modulo p.*

Proof. Fix a prime p and for any $d \in \mathbb{N}$ such that $d \mid (p-1)$ define

$$A(d) = \{a \in \mathbb{N} : 1 \leq a \leq p-1,\ \mathrm{ord}_p(a) = d\}.$$

Let $\psi(d) = \#A(d) \geq 0$. We aim to show that $\psi(d) = \varphi(d)$.

Since the sets $A(d)$ partition $\{1, 2, \ldots, p-1\}$ we have

$$\sum_{d \mid (p-1)} \psi(d) = p - 1.$$

By Proposition 2.48 we also have

$$\sum_{d \mid (p-1)} \varphi(d) = p - 1.$$

Therefore if we can show that $\psi(d) \leq \varphi(d)$ for all $d \mid (p-1)$ then $\psi(d) = \varphi(d)$ for all such d. (Otherwise, if $\psi(d_0) < \varphi(d)$ for some d_0, then $\sum_{d \mid (p-1)} \psi(d) < \sum_{d \mid (p-1)} \phi(d)$ - contradiction.)

If $\psi(d) = 0$ then $\psi(d) \leq \varphi(d)$ and so we are done. So we are reduced to considering the case $\psi(d) \geq 1$. Then $A(d) \neq \emptyset$ and so $a \in A(d)$ for some a. Hence $\mathrm{ord}_p(a) = d$ and so $a^d \equiv 1 \bmod p$. Then $(a^i)^d \equiv 1 \bmod p$ for all $i \in \mathbb{Z}$. In particular, the d numbers

$$a, a^2, \ldots, a^d \tag{14}$$

are solutions of the polynomial congruence

$$x^d - 1 \equiv 0 \bmod p. \tag{15}$$

By Corollary 2.55 the numbers listed in (14) are incongruent mod p since $\mathrm{ord}_p(a) = d$. Moreover, (15) has at most d solutions by Lagrange's polynomial congruence theorem (Theorem 2.68). Therefore the d numbers in (14) must be *all* the solutions of (15) mod p. Hence each number in $A(d)$ must be congruent to a^k mod p for some $k = 1, \ldots, d$. By Lemma 2.83 $\mathrm{ord}_p(a^k) = d$ if and only if $\gcd(k, d) = 1$. In other words, among the d numbers in (14) there are $\varphi(d)$ which have order d modulo p. Thus we have shown that $\psi(d) = \varphi(d)$ if $\psi(d) \neq 0$, as required. □

Example 2.86. There are $\varphi(19-1) = \varphi(18) = 6$ primitive roots mod 19. Thus there are $\varphi(19) - 6 = 12$ elements of $(\mathbb{Z}/19\mathbb{Z})^\times$ that are not primitive roots.

Corollary 2.87. *Let p be prime. Then there exists a primitive root g modulo p (note that g need not be unique). In other words, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. Moreover, for any $a \in \mathbb{Z}$ with $p \nmid a$ there exists $k \in \mathbb{Z}$ such that $a \equiv g^k \bmod p$.*

Proof. The existence of a primitive root follows from Theorem 2.85 since $\varphi(p-1) \geq 1$. By definition of primitive root, $\operatorname{ord}_p(g) = p-1$ and so $1, g, g^2, \ldots, g^{p-2}$ are congruent modulo p, in some order, to $1, 2, \ldots, p-1$ (use Corollary 2.55), which gives the last claim. □

Theorem 2.88 (The primitive root test)**.** *Let $n \in \mathbb{N}$ and let $a \in \mathbb{Z}$ with* $\gcd(a,n) = 1$*. Then a is a primitive root modulo n if and only if*

$$a^{\varphi(n)/q} \not\equiv 1 \bmod n$$

for every prime q dividing $\varphi(n)$.

Proof. If $a^{\varphi(n)/q} \equiv 1 \bmod n$ for some prime q dividing $\varphi(n)$ then $\operatorname{ord}_n(a) \leq \varphi(n)/q < \varphi(n)$ and so a cannot be a primitive root mod n.

Suppose conversely that $a^{\varphi(n)/q} \not\equiv 1 \bmod n$ for every prime q dividing $\varphi(n)$. Write $\varphi(n) = q_1^{r_1} \cdots q_s^{r_s}$ where the q_i's are distinct primes and each $r_i \in \mathbb{N}$. Let $m = \operatorname{ord}_n(a)$. Then $m \mid \varphi(n)$ by Corollary 2.60 and so $m = q_1^{t_1} \cdots q_s^{t_s}$ where for each i we have $0 \leq t_i \leq r_i$. Suppose $m < \varphi(n)$. Then there exists a j such that $t_j < r_j$. Hence m divides $q_1^{r_1} \cdots q_j^{r_j - 1} \cdots q_s^{r_s} = (\varphi(n)/q_j)$. But $a^m \equiv 1 \bmod n$ and so $a^{\varphi(n)/q_j} \equiv 1 \bmod n$, contradicting our hypothesis. □

Example 2.89. Find a primitive root modulo 31. Since 31 is prime, we have $\varphi(31) = 31 - 1 = 30 = 2 \times 3 \times 5$. Thus given $a \in \mathbb{Z}$ with $31 \nmid a$ we need to check that

$$a^{15} \not\equiv 1 \bmod 31, \quad a^{10} \not\equiv 1 \bmod 31, \quad \text{and} \quad a^6 \not\equiv 1 \bmod 31$$

Try $a = 2$. Then $2^{10} \equiv (2^5)^2 \equiv 32^2 \equiv 1^2 \equiv 1 \bmod 31$. Thus 2 is not a primitive root mod31.

Try $a = 3$. First note that $3^5 = 243 \equiv -5 \mod 31$. Then we have

- $3^6 = 3^5 \times 3 \equiv -5 \times 3 \equiv -15 \equiv 16 \not\equiv 1 \bmod 31$.
- $3^{10} = (3^5)^2 \equiv (-5)^2 \equiv 25 \not\equiv 1 \bmod 31$.
- $3^{15} = 3^5 \times 3^{10} \equiv -5 \times 25 \equiv -125 \equiv -1 \not\equiv 1 \bmod 31$.

Therefore 3 is a primitive root modulo 31.

Theorem 2.90. *Let p be an odd prime. If g is a primitive root* mod p *then g is also a primitive root mod p^e for all $e \geq 1$ if and only if $g^{p-1} \not\equiv 1 \bmod p^2$.*

Proof. Not examinable (but statement *is* examinable). See Apostal, *Introduction to Analytic Number Theory*, Chapter 10, for example. □

Theorem 2.91. *Let $n \in \mathbb{N}$. Then $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic $\Leftrightarrow$ there exists a primitive root modulo n $\Leftrightarrow$ $n = 1, 2, 4, p^e, 2p^e$ where $e \in \mathbb{N}$ and p is an odd prime.*

Proof. Not examinable (but statement *is* examinable). See Apostal, *Introduction to Analytic Number Theory*, Chapter 10, for example. □

2.13 Wilson's Theorem

Theorem 2.92 (Wilson's Theorem)**.** *An integer $p \geq 2$ is prime if and only if $(p-1)! \equiv -1 \bmod p$.*

Example 2.93. For $p = 5$, we have $(5-1)! = 4! = 24 \equiv -1 \bmod 5$; but for $p = 6$, we have $(6-1)! = 5! = 120 \equiv 0 \bmod 6$.

Proof. Suppose n is composite. Then there exists d dividing n with $1 < d < n$. Therefore $d \mid (n-1)!$ and $d \mid n$. So if $(n-1)! \equiv -1 \bmod n$ then $n \mid ((n-1)!+1)$ and so $d \mid ((n-1)!+1)$. Hence $d \mid 1 = ((n-1)!+1)-(n-1)!$. Contradiction. Hence $(n-1)! \not\equiv -1 \bmod n$.

Suppose p is prime. The case $p = 2$ is easy, so we can and do assume that p is odd. Each a in $\{1, 2, \dots, p-1\}$ is coprime to p and therefore has a unique *inverse* $a^{-1} \in \{1, 2, \dots, p-1\}$ modulo p, that is $aa^{-1} \equiv 1 \bmod p$. Note that $(a^{-1})^{-1} \equiv a \bmod p$. If $a = a^{-1}$ then $1 \equiv aa^{-1} = a^2 \bmod p$. By Corollary 2.71 we then have $a \equiv \pm 1 \bmod p$ and so $a = 1$ or $a = p-1$. In the product

$$(p-1)! = 1 \times 2 \times 3 \times \cdots \times (p-2) \times (p-1)$$

we pair off each term, save for 1 and $p-1$, with its inverse modulo p. We thus have $(p-1)! \equiv 1 \times (p-1) \equiv -1 \bmod p$. □

Example 2.94. As an illustration, consider the case $p = 11$. Then

$$\begin{aligned} 10! &= 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \\ &= 1 \times (2 \times 6) \times (3 \times 4) \times (5 \times 9) \times (7 \times 8) \times 10 \\ &\equiv 1 \times 1 \times 1 \times 1 \times 1 \times 10 = 10 \equiv -1 \bmod 11. \end{aligned}$$

Alternative proof of Wilson's Theorem using primitive roots. If n is composite we proceed as before. Again, we are reduced to considering the case where p is an odd prime. Let g be a primitive root modulo p (this exists by Corollary 2.87). Then the numbers 1, g, $g^2, \dots, g^{p-2}$ are congruent modulo p, in some order, to 1, $2, \dots, p-1$. Hence

$$(p-1)! \equiv 1gg^2 \cdots g^{p-2} = g^{1+2+\cdots+(p-2)} \bmod p.$$

The sum $1 + 2 + \cdots + (p-2)$ is the sum of an arithmetic progression with $p-2$ terms, and so equals

$$(p-2)\frac{(p-2)+1}{2} = \frac{(p-2)(p-1)}{2}.$$

Hence

$$(p-1)! \equiv g^{(p-2)(p-1)/2} \bmod p.$$

Since p is odd we have $p = 2k + 1$ for some $k \in \mathbb{N}$. As $k < 2k = p - 1$ then $g^k \not\equiv 1 \pmod{p}$ but $g^{2k} = g^{p-1} \equiv 1 \pmod{p}$ because $\operatorname{ord}_p(g) = p - 1$ by definition of g (or use Fermat's little theorem). Since $(g^k)^2 = g^{2k} \equiv 1 \bmod p$ we have $g^k \equiv \pm 1 \bmod p$ by Corollary 2.71. Hence $g^k \equiv -1 \bmod p$. We finally conclude that

$$(p-1)! \equiv g^{(p-2)(p-1)/2} = g^{(2k-1)k} = (g^k)^{2k-1} \equiv (-1)^{2k-1} = -1 \bmod p. \quad \square$$

3 Quadratic Residues

3.1 Quadratic Residues

We shall study the theory of quadratic congruences modulo an odd prime p. By the familiar technique of completing the square one can reduce any such congruence to the form

$$x^2 \equiv a \bmod p.$$

Example 3.1. Consider the case $p = 11$.

x	0	1	2	3	4	5	6	7	8	9	10
x^2 mod 11	0	1	4	9	5	3	3	5	9	4	1

Notice the symmetry in this table. This is because for any odd prime p and any $k \in \mathbb{Z}$ we have $(p-k)^2 \equiv (-k)^2 \equiv k^2 \bmod p$. For example, $3^2 \equiv (-3)^2 \equiv (11-3)^2 \equiv 8^2 \bmod 11$. Also notice that

$$x^2 \equiv a \bmod 11 \text{ has } \begin{cases} \text{one solution if } a \equiv 0 \bmod 11, \\ \text{two solutions if } a \equiv 1, 3, 4, 5, 9 \bmod 11, \\ \text{no solutions if } a \equiv 2, 6, 7, 8, 10 \bmod 11. \end{cases}$$

Lemma 3.2. *Let p be an odd prime and let $a \in \mathbb{Z}$. Consider*

$$x^2 \equiv a \bmod p. \tag{16}$$

If $p \mid a$ then (16) *is equivalent to $x \equiv 0 \bmod p$. Otherwise, if $p \nmid a$ and* (16) *has a solution $x \equiv b \bmod p$ then $p \nmid b$ and $x \equiv -b$ is another, different solution.*

Proof. If $x \equiv 0 \bmod p$ then clearly $x^2 \equiv 0 \bmod p$. The converse follows from Euclid's Lemma for Primes (Theorem 1.23): if $x^2 \equiv 0 \bmod p$ then $p \mid x^2$ so we must have $p \mid x$, i.e., $x \equiv 0 \bmod p$.

Suppose that $p \nmid a$ and $b^2 \equiv a \bmod p$. Then clearly $(-b)^2 \equiv b^2 \equiv a \bmod p$. If $b \equiv -b \bmod p$ then $2b \equiv 0 \bmod p$ so $b \equiv 0 \bmod p$ by the Cancellation Law for Congruences (Theorem 2.11) since p is odd. But then $a \equiv b^2 \equiv 0 \bmod p$, contradicting the assumption that $p \nmid a$. $\square$

Definition 3.3. Let p be an odd prime, and suppose we have $a \in \mathbb{Z}$ such that $p \nmid a$. Then a is a *Quadratic Residue* of p if there exists $x \in \mathbb{Z}$ such that $x^2 \equiv a \bmod p$, and a is *Quadratic Non-Residue* if not.

Proposition 3.4. *Let p be an odd prime. Then every reduced residue system mod p contains exactly $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic non-residues mod p. The quadratic residues belong to the residue classes containing the numbers*

$$1^2, 2^2, 3^2, \ldots, ((p-1)/2)^2. \tag{17}$$

Proof. First we show that the list of numbers in (17) are distinct mod p. Indeed, if $x^2 \equiv y^2 \bmod p$ with $1 \le x \le (p-1)/2$ and $1 \le y \le (p-1)/2$ then

$$(x-y)(x+y) \equiv 0 \bmod p.$$

But $1 < (x+y) < p$ so $(x+y)$ is coprime to p. So by the Cancellation Law for Congruences (Theorem 2.11) we must have $(x-y) \equiv 0 \bmod p$, hence $x \equiv y \bmod p$ and so $x = y$ (by Proposition 2.14). The remaining squares are

$$((p+1)/2)^2, ((p+3)/2)^2, \ldots, (p-2)^2, (p-1)^2.$$

Since $(p-k)^2 \equiv (-k)^2 \equiv k^2 \bmod p$ for every $k \in \mathbb{Z}$ with $1 \le k \le (p-1)/2$, these are congruent to

$$((p-1)/2)^2, ((p-3)/2)^2, \ldots, 2^2, 1^2.$$

These are precisely the numbers in (17). Hence there are precisely $(p-1)/2$ quadratic residues mod p, and so there are $(p-1) - (p-1)/2 = (p-1)/2$ quadratic non-residues mod p. □

3.2 The Legendre Symbol

Definition 3.5. Let p be an odd prime. For any $a \in \mathbb{Z}$, we define the *Legendre Symbol* to be

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & p \nmid a \text{ and } a \text{ is a quadratic residue of } p, \\ -1, & p \nmid a \text{ and } a \text{ is a quadratic non-residue of } p, \\ 0, & p \mid a. \end{cases}$$

Remark 3.6. By Lemma 3.2 we see that the congruence $x^2 \equiv a \bmod p$ has precisely $\left(\frac{a}{p}\right) + 1$ distinct solutions modulo p.

Remark 3.7. Note that we always have $\left(\frac{1}{p}\right) = 1$. Moreover, if $a, b \in \mathbb{Z}$ with $a \equiv b \bmod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ (this is sometimes known as periodicity).

Examples 3.8. $\left(\frac{5}{11}\right) = 1$, $\left(\frac{7}{11}\right) = -1$, $\left(\frac{22}{11}\right) = 0$.
If $m \in \mathbb{Z}$ with $p \nmid m$ then $\left(\frac{m^2}{p}\right) = 1$.

3.3 Euler's Criterion

Lemma 3.9. *Let p be an odd prime and let g be a primitive root mod p. Let $a \in \mathbb{Z}$ with $p \nmid a$. Then $a \equiv g^k \bmod p$ for some $k \in \mathbb{Z}$ and a is a quadratic residue mod p if and only if k is even.*

Proof. First note that a primitive root $g \bmod p$ exists by Corollary 2.87, so $a \equiv g^k \bmod p$ for some $k \in \mathbb{Z}$. Suppose k is even. Then $k = 2j$ for some $j \in \mathbb{Z}$ and so $a \equiv (g^j)^2 \bmod p$. Thus a is a quadratic residue mod p. Suppose conversely that a is quadratic residue mod p. Then $a \equiv b^2 \bmod p$ for some $b \in \mathbb{Z}$ with $p \nmid b$. Then $b \equiv g^r$ for some $r \in \mathbb{Z}$ and so $g^k \equiv (g^r)^2 \equiv g^{2r} \bmod p$. Thus $k \equiv 2r \bmod p-1$ by Proposition 2.53 since $\operatorname{ord}_p(g) = \varphi(p) = p-1$. So $k \equiv 2r \bmod 2$ since $2 \mid (p-1)$. Hence $k \equiv 0 \bmod 2$, i.e., k must be even. □

Theorem 3.10 (Euler's Criterion)**.** *If p is an odd prime and $a \in \mathbb{Z}$ then*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Proof. This is obvious if $p \mid a$. So suppose that $p \nmid a$. Let g be a primitive root mod p. Then there exists $k \in \mathbb{Z}$ such that $a \equiv g^k \bmod p$. Since $\operatorname{ord}_p(g) = p-1$ we have $g^{p-1} \equiv 1 \bmod p$ and $g^{(p-1)/2} \not\equiv 1 \bmod p$. But Corollary 2.71 says that $g^{(p-1)/2} \equiv \pm 1 \bmod p$. Therefore $g^{(p-1)/2} \equiv -1 \bmod p$. Then

$$a^{(p-1)/2} \equiv (g^k)^{(p-1)/2} \equiv (g^{(p-1)/2})^k \equiv (-1)^k \bmod p.$$

The result now follows from Lemma 3.9. □

Alternative proof of Euler's Criterion. Again, we may suppose that $p \nmid a$. Suppose that $\left(\frac{a}{p}\right) = 1$. Then there exists $b \in \mathbb{Z}$ with $p \nmid b$ such that $a \equiv b^2 \bmod p$. Thus by Fermat's Little Theorem (Corollary 2.62) we have

$$a^{(p-1)/2} \equiv (b^2)^{(p-1)/2} \equiv b^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) \bmod p.$$

Now suppose that $\left(\frac{a}{p}\right) = -1$ and consider the polynomial

$$f(x) = x^{(p-1)/2} - 1.$$

Since $f(x)$ has degree $(p-1)/2$, Lagrange's polynomial congruence theorem (Theorem 2.68) says that the congruence

$$f(x) \equiv 0 \bmod p$$

has at most $(p-1)/2$ solutions. But we have shown that the quadratic residues mod p are solutions, and Proposition 3.4 says there are $(p-1)/2$ of them. Hence none of the quadratic non residues are solutions and so $a^{(p-1)/2} \not\equiv 1 \bmod p$. But by Fermat's Little Theorem (Corollary 2.62) we have $a^{(p-1)} \equiv 1 \bmod p$ and so by Corollary 2.71 $a^{(p-1)/2} \equiv \pm 1 \bmod p$. Therefore

$$a^{(p-1)/2} \equiv -1 \equiv \left(\frac{a}{p}\right) \bmod p.$$

This completes the proof. □

Theorem 3.11 (Multiplicativity of the Legendre Symbol)**.** *Let p be an odd prime. Let $a, b \in \mathbb{Z}$. Then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*

Proof. If $p \mid a$ or $p \mid b$ then $p \mid ab$ so $\left(\frac{ab}{p}\right) = 0$ and either $\left(\frac{a}{p}\right) = 0$ or $\left(\frac{b}{p}\right) = 0$. Hence we have the desired result in this case.

Suppose $p \nmid a$ and $p \nmid b$. Then by Euclid's Lemma for Primes we have $p \nmid ab$. Moreover, by Euler's Criterion we have

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p,$$

and both sides are 1 or -1. If they were different, we would have $+1 \equiv -1 \bmod p$ and so $p \mid 2$, which gives a contradiction as p is odd. □

Theorem 3.12. *If p is an odd prime then*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & p \equiv 1 \bmod 4, \\ -1, & p \equiv 3 \bmod 4. \end{cases}$$

In other words, $x^2 \equiv -1 \bmod p$ is soluble if and only if $p \equiv 1 \bmod 4$.

Proof. By Euler's Criterion we have

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p,$$

and both sides are $+1$ or -1. If they were different, we would have $+1 \equiv -1 \bmod p$ and so $p \mid 2$, which gives a contradiction as p is odd. □

Example 3.13. Can we solve $x^2 \equiv 13 \bmod 17$?

$$\begin{aligned}
\left(\frac{13}{17}\right) &= \left(\frac{-4}{17}\right) && \text{by periodicity (Remark 3.7)} \\
&= \left(\frac{-1}{17}\right)\left(\frac{2}{17}\right)\left(\frac{2}{17}\right) && \text{by multiplicativity (Theorem 3.11)} \\
&= \left(\frac{-1}{17}\right) && \text{as } (\pm 1)^2 = 1 \\
&= (-1)^{(17-1)/2} && \text{since } 17 \equiv 1 \bmod 4 \text{ (use Theorem 3.12)} \\
&= (-1)^8 = 1
\end{aligned}$$

Hence the congruence is soluble! Note that this proof that a solution exists cannot be adapted to provide a concrete solution. It is purely an existence argument.

Theorem 3.14. *There are infinitely many primes p with $p \equiv 1 \bmod 4$.*

Proof. It suffices to show that for any $N \in \mathbb{N}$ there exists a prime p with $p > N$ and $p \equiv 1 \bmod 4$. Let $M = (2(N!))^2 + 1$. If p is a prime with $p \leq N$ then $M \equiv 1 \bmod p$ and so $p \nmid M$. Let p be a prime factor of M. Then $p > N$. As M is odd, p is also odd. Then we have $(2(N!))^2 \equiv -1 \bmod p$ and so the congruence $x^2 \equiv -1 \bmod p$ is soluble. Therefore $p \equiv 1 \bmod 4$ by Theorem 3.12. □

3.4 Gauss' Lemma

Definition 3.15. Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$. We write $\lambda(a, n)$ for the unique integer such that $a \equiv \lambda(a, n) \bmod n$ and $0 \leq \lambda(a, n) < n$. In other words, $\lambda(a, n)$ is the remainder when the Division Algorithm is applied to a and n. (This is not a standard notation, and is intended merely for temporary use in our discussion of quadratic residues.)

Theorem 3.16 (Gauss' Lemma). *Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Then*

$$\left(\frac{a}{p}\right) = (-1)^{\Lambda} \text{ where } \Lambda := \#\{j \in \mathbb{N} : 1 \leq j \leq \tfrac{p-1}{2}, \lambda(aj, p) > \tfrac{p}{2}\}.$$

Example 3.17. Let $p = 13$ and $a = 5$.
If $j = 1$ then $\lambda(aj, p) = \lambda(5, 13) = 5 < 13/2$.
If $j = 2$ then $\lambda(aj, p) = \lambda(10, 13) = 10 > 13/2$.
If $j = 3$ then $\lambda(aj, p) = \lambda(15, 13) = 2 < 13/2$.

If $j = 4$ then $\lambda(aj, p) = \lambda(20, 13) = 7 > 13/2$.
If $j = 5$ then $\lambda(aj, p) = \lambda(25, 13) = 12 > 13/2$.
If $j = 6$ then $\lambda(aj, p) = \lambda(30, 13) = 4 < 13/2$.
Hence $\Lambda = \#\{2, 4, 5\} = 3$ and so $\left(\frac{5}{13}\right) = (-1)^3 = -1$.

Proof. Let $S_a := \{aj : 1 \leq j \leq \frac{p-1}{2}\}$ and define

$$\{r_1, \ldots, r_m\} = \{\lambda(aj, p) : aj \in S_a,\ 0 < \lambda(aj, p) < \tfrac{p}{2}\},$$

$$\{s_1, \ldots, s_n\} = \{\lambda(aj, p) : aj \in S_a, \tfrac{p}{2} < \lambda(aj, p) < p\},$$

so that $n = \Lambda$. Note that $\lambda(aj, p) \neq \frac{p}{2}$ since $\frac{p}{2} \notin \mathbb{Z}$ and that $\lambda(aj, p) \neq 0$, since $p \nmid a$ and $p \nmid j$. Also note that if $j_1 \neq j_2$ then $\lambda(aj_1, p) \neq \lambda(aj_2, p)$ since

$$\begin{aligned}\lambda(aj_1, p) = \lambda(aj_2, p) &\implies aj_1 \equiv aj_2 \bmod p\\ &\implies j_1 \equiv j_2 \bmod p \text{ (by cancellation law; note } p \nmid a)\\ &\implies j_1 = j_2 \ \text{ (since } 0 < j_1, j_2 < p).\end{aligned}$$

Hence $m + n = \#S_a = \frac{p-1}{2}$. We claim that

$$\{r_1, \ldots, r_m, (p - s_1), \ldots, (p - s_n)\} = \{1, 2, \ldots, \tfrac{p-1}{2}\}.$$

Clearly $r_i, (p - s_j) \in \{1, 2, \ldots, \frac{p-1}{2}\}$ and there are $\frac{p-1}{2}$ elements $r_i, (p - s_j)$, so it suffices to show that they are all different. We have already shown that $r_i \neq r_j$ and $s_i \neq s_j$ for $i \neq j$. To show that $r_i \neq p - s_j$ we argue by contradiction. If $r_i + s_j = p$, let $r_i = \lambda(aj_1, p)$ and $s_j = \lambda(aj_2, p)$. Then

$$r_i + s_j = p = \lambda(aj_1, p) + \lambda(aj_2, p) \equiv aj_1 + aj_2 \equiv a(j_1 + j_2) \bmod p.$$

Hence $a(j_1 + j_2) \equiv 0 \bmod p$. So by Euclid's lemma for primes, either $p \mid a$ or $p \mid (j_1 + j_2)$. However, $p \nmid a$ by assumption and $2 \leq j_1 + j_2 \leq p - 1$ so that $p \nmid (j_1 + j_2)$ - contradiction. Therefore $r_i \neq p - s_j$, which proves the claim.

Now, on the one hand, we have

$$\begin{aligned}r_1 r_2 \cdots r_m (p - s_1) \cdots (p - s_n) &= 1 \times 2 \times \cdots \times \tfrac{p-1}{2} = \left(\tfrac{p-1}{2}\right)!\\ &\equiv r_1 r_2 \cdots r_m s_1 s_2 \cdots s_n (-1)^n \bmod p.\end{aligned}$$

On the other hand, by the definition of r_i, s_j,

$$r_1 r_2 \cdots r_m s_1 s_2 \cdots s_n = \prod_{j=1}^{\frac{p-1}{2}} \lambda(aj, p) \equiv \prod_{j=1}^{\frac{p-1}{2}} (aj) = a^{\frac{p-1}{2}} \left(\tfrac{p-1}{2}\right)! \bmod p.$$

Therefore

$$\left(\tfrac{p-1}{2}\right)! \equiv (-1)^n a^{\frac{p-1}{2}} \left(\tfrac{p-1}{2}\right)! \bmod p.$$

Now, since $p \nmid \left(\frac{p-1}{2}\right)!$, the cancellation law for congruences shows that

$$1 \equiv (-1)^n a^{\frac{p-1}{2}} \bmod p.$$

Thus $a^{\frac{p-1}{2}} \equiv (-1)^n \bmod p$ and so $\left(\frac{a}{p}\right) \equiv (-1)^n \bmod p$ by Euler's Criterion (Theorem 3.10). Both sides are $+1$ or -1 and if they were different, we would have $+1 \equiv -1 \bmod p$ and so $p \mid 2$, which gives a contradiction as p is odd. Therefore $\left(\frac{a}{p}\right) = (-1)^n = (-1)^\Lambda$ as required. □

Definition 3.18. For any $x \in \mathbb{R}$ we set $\lfloor x \rfloor := \max\{n \in \mathbb{Z} : n \leq x\}$. For example, $\lfloor 3 \rfloor = 3$, $\lfloor \pi \rfloor = 3$ and $\lfloor -\pi \rfloor = -4$.

Corollary 3.19. *If p is an odd prime then*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} +1, & p \equiv \pm 1 \bmod 8, \\ -1, & p \equiv \pm 3 \bmod 8. \end{cases}$$

Proof. We shall apply Gauss' Lemma (Theorem 3.16) for $a = 2$, so that

$$\left(\frac{2}{p}\right) = (-1)^\Lambda \text{ where } \Lambda = \#\{1 \leq j \leq \tfrac{p-1}{2} : \lambda(2j,p) > \tfrac{p}{2}\}.$$

Note that for $1 \leq j \leq \frac{p-1}{2}$ we have $2 \leq 2j \leq p-1$ and so $\lambda(2j,p) = 2j$. Moreover, $2j < \frac{p}{2}$ if and only if $j < \frac{p}{4}$, and $\frac{p}{2} < 2j < p$ if and only if $\frac{p}{4} < j < \frac{p}{2}$. It follows that $\Lambda = \#\{j \in \mathbb{N} : \frac{p}{4} < j < \frac{p}{2}\}$. We have

$$\#\left\{j : \tfrac{p}{4} < j < \tfrac{p}{2}\right\} = \#\left\{j \leq \tfrac{p-1}{2}\right\} - \#\left\{j < \tfrac{p}{4}\right\} = \tfrac{p-1}{2} - \left\lfloor \tfrac{p}{4} \right\rfloor.$$

Since p is odd, precisely one of the following cases must occur:

(i) $p = 8k+1 \implies \frac{p-1}{2} = 4k,\ \left\lfloor \frac{p}{4} \right\rfloor = 2k \implies \Lambda = 2k,$

(ii) $p = 8k+3 \implies \frac{p-1}{2} = 4k+1,\ \left\lfloor \frac{p}{4} \right\rfloor = 2k \implies \Lambda = 2k+1,$

(iii) $p = 8k+5 \implies \frac{p-1}{2} = 4k+2,\ \left\lfloor \frac{p}{4} \right\rfloor = 2k+1 \implies \Lambda = 2k+1,$

(iv) $p = 8k+7 \implies \frac{p-1}{2} = 4k+3,\ \left\lfloor \frac{p}{4} \right\rfloor = 2k+1 \implies \Lambda = 2k+2.$

Hence

$$(-1)^\Lambda = +1 \iff p = 8k+1 \text{ or } 8k+7 \iff p \equiv \pm 1 \bmod 8.$$

We note that if $p = 8k+r$ then

$$\frac{p^2-1}{8} = \frac{r^2+16rk+64k^2-1}{8} = \frac{r^2-1}{8} + 2(kr+4k^2) \equiv \frac{r^2-1}{8} \bmod 2.$$

By checking the cases $r = \pm 1, \pm 3$ we deduce that

$$\frac{p^2-1}{8} \equiv \begin{cases} 0 \bmod 2, & p \equiv \pm 1 \bmod 8, \\ 1 \bmod 2, & p \equiv \pm 3 \bmod 8, \end{cases}$$

and the result follows. □

Example 3.20. Since $1009 \equiv 1 \bmod 8$ we have $\left(\frac{2}{1009}\right) = 1$. Since $1997 \equiv -3 \bmod 8$ we have $\left(\frac{2}{1997}\right) = -1$. (Note that 1009 and 1997 are both prime.)

Theorem 3.21. *There are infinitely many primes p with $p \equiv -1 \bmod 8$.*

Proof. It suffices to show that for any $N \in \mathbb{N}$ there exists a prime p with $p > N$ and $p \equiv -1 \bmod 8$. Let $M = 8(N!)^2 - 1$. If p is a prime with $p \leq N$ then $M \equiv -1 \bmod p$ and so $p \nmid M$.

Let p be a prime factor of M. Then p is odd and $p > N$. Moreover,

$$(4(N!))^2 \equiv 16(N!)^2 \equiv 2M + 2 \equiv 2 \bmod p.$$

Thus $\left(\frac{2}{p}\right) = +1$ and so $p \equiv \pm 1 \bmod 8$ by Corollary 3.19. But if all prime factors of M were congruent to 1 mod 8, then we would have $M \equiv 1 \bmod 8$, which is not the case. Therefore M must have at least one prime factor p with $p \equiv -1 \bmod 8$ and $p > N$. □

Lemma 3.22. *Let p be an odd prime and let $a \in \mathbb{Z}$ with a odd and $p \nmid a$. Then*

$$\left(\frac{a}{p}\right) = (-1)^t \text{ where } t = \sum_{k=1}^{(p-1)/2} \lfloor ak/p \rfloor .$$

Proof. Recall the notation from the proof of Gauss' Lemma (Theorem 3.16). For any $j \in \mathbb{Z}$ we have $\lambda(aj, p) \equiv aj \bmod p$, with $0 \leq \lambda(aj, p) < p$. Here $\lambda(aj, p) = aj - pk$ for some $k \in \mathbb{Z}$ such that $0 \leq aj - pk < p$. It follows that $k \leq \frac{aj}{p} < k + 1$, and hence that $k = \left\lfloor \frac{aj}{p} \right\rfloor$. We therefore deduce that $\lambda(aj, p) = aj - p \left\lfloor \frac{aj}{p} \right\rfloor$. Using this expression we now have

$$\sum_{i=1}^{m} r_i + \sum_{i=1}^{n} s_i = \sum_{j=1}^{(p-1)/2} \lambda(aj, p) = \sum_{j=1}^{(p-1)/2} \left(aj - p \left\lfloor \frac{aj}{p} \right\rfloor \right).$$

Hence, since a and p are odd, we have

$$\sum_{j=1}^{(p-1)/2} j - \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{aj}{p} \right\rfloor \equiv \sum_{i=1}^{m} r_i + \sum_{i=1}^{n} s_i \bmod 2, \quad (*).$$

Recall from the proof of Gauss' Lemma (Theorem 3.16) that

$$\{r_1, \ldots, r_m, (p - s_1), \ldots, (p - s_n)\} = \{1, 2, \ldots, \tfrac{p-1}{2}\}.$$

Thus

$$\sum_{i=1}^{m} r_i + np + \sum_{i=1}^{n} s_i \equiv \sum_{j=1}^{(p-1)/2} j \bmod 2,$$

and hence

$$\sum_{i=1}^{m} r_i + \sum_{i=1}^{n} s_i \equiv n + \sum_{j=1}^{(p-1)/2} j \bmod 2.$$

Comparing this with $(*)$, we see that

$$n \equiv \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{aj}{p} \right\rfloor \bmod 2,$$

and the result follows from Gauss' Lemma (Theorem 3.16). □

3.5 The Law of Quadratic Reciprocity

Theorem 3.23 (The Law of Quadratic Reciprocity - LQR)**.** *If p and q are distinct odd primes, then*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} = \begin{cases} +\left(\frac{q}{p}\right), & \textit{if } p \equiv 1 \bmod 4 \ \textit{ or } \ q \equiv 1 \bmod 4, \\ -\left(\frac{q}{p}\right), & \textit{if } p \equiv q \equiv 3 \bmod 4. \end{cases}$$

Proof. To prove the Law of Quadratic Reciprocity it suffices, by Lemma 3.22, to show that

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{qk}{p} \right\rfloor + \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{pk}{q} \right\rfloor = \frac{p-1}{2} \times \frac{q-1}{2}.$$

We shall count the points in

$$R := \left\{(x,y) \in \mathbb{N} \times \mathbb{N} : 0 < x < \tfrac{p}{2},\, 0 < y < \tfrac{q}{2}\right\}$$

in two different ways. First note that since p and q are odd, we have

$$\#R = \#\{x : 0 < x < \tfrac{p}{2}\} \times \#\{y : 0 < y < \tfrac{q}{2}\} = \tfrac{p-1}{2} \times \tfrac{q-1}{2}.$$

We now find another expression for $\#R$. If a point (x,y) were on the line from $(0,0)$ to $(\frac{p}{2}, \frac{q}{2})$ we would have $y = \frac{qx}{p}$ and hence $py = qx$. However, then we would have $p \mid qx$, which is impossible by Euclid's lemma for primes, since $p \nmid q$ and $p \nmid x$ (recall that $0 < x < p/2$). Thus there are no points (x,y) of R on the line from $(0,0)$ to $(\frac{p}{2}, \frac{q}{2})$.

How many points (x, y) of R are there below (or on) the diagonal? For each value of x with $1 \leq x \leq \frac{p-1}{2}$, the pairs (x, y) below the diagonal must satisfy $1 \leq y \leq \frac{q}{p}x$. However, there are $\lfloor \frac{qx}{p} \rfloor$ such values of y. It follows that the total number of points below (or on) the line $y = qx/p$ is

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{qk}{p} \right\rfloor.$$

Similarly, there are

$$\sum_{k=1}^{(q-1)/2} \left\lfloor \frac{pk}{q} \right\rfloor$$

points above (or on) the line. It follows that

$$\#R = \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{qk}{p} \right\rfloor + \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{pk}{q} \right\rfloor.$$

Comparing the two expressions for $\#R$ gives the result. □

Example 3.24. What is $\left(\frac{29}{53}\right)$? In other words, can we solve $x^2 \equiv 29 \bmod 53$? Note that 29 and 53 are both prime. Use LQR:

$$\begin{aligned}
\left(\frac{29}{53}\right) &= \left(\frac{53}{29}\right) \quad \text{(by LQR since } 29 \equiv 1 \bmod 4) \\
&= \left(\frac{24}{29}\right) \quad \text{(by periodicity since } 53 \equiv 24 \bmod 29) \\
&= \left(\frac{2 \times 2 \times 2 \times 3}{29}\right) \\
&= \left(\frac{2}{29}\right)^3 \left(\frac{3}{29}\right) \quad \text{(by multiplicativity).}
\end{aligned}$$

We now use LQR and Corollary 3.19 repeatedly:

$$\begin{aligned}
\left(\frac{2}{29}\right) &= -1 \quad \text{(by Corollary 3.19 since } 29 \equiv -3 \bmod 8) \\
\left(\frac{3}{29}\right) &= \left(\frac{29}{3}\right) \quad \text{(by LQR since } 29 \equiv -3 \bmod 4) \\
&= \left(\frac{2}{3}\right) \quad \text{(by periodicity since } 29 \equiv 2 \bmod 3) \\
&= -1 \quad \text{(by Corollary 3.19 since } 3 \equiv 3 \bmod 8).
\end{aligned}$$

Thus $\left(\frac{29}{53}\right) = (-1)^4 = +1$, and hence $x^2 \equiv 29 \bmod 53$ is soluble.

Example 3.25. Recall that in Example 2.67 we used the binary powering algorithm to show that $3^{499} \equiv 3 \bmod 997$.

We now perform this computation in a different way. Note that 997 is a prime and that $997 \equiv 1 \bmod 4$. Moreover, $997 \equiv 1 \bmod 3$. Hence by LQR we have

$$\left(\frac{3}{997}\right) = \left(\frac{997}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

However, Euler's Criterion (Theorem 3.10) gives

$$\left(\frac{3}{997}\right) \equiv 3^{(997-1)/2} \equiv 3^{498} \bmod 997.$$

Hence $3^{498} \equiv 1 \bmod 997$ and so $3^{499} \equiv 3 \bmod 997$.

Note that we were "lucky" with the choice of exponent here in that is was close to $(997-1)/2$. In general, if p is prime and $a \in \mathbb{Z}$ with $p \nmid a$ then we can use LQR and Euler's Criterion to compute $a^{(p-1)/2} \bmod p$. (In particular, we must have $a^{(p-1)/2} \equiv \pm 1 \bmod p$.)

Example 3.26. Determine $\left(\frac{3}{p}\right)$ where $p \geq 5$ is a prime.

By LQR we have

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{(p-1)(3-1)/4} = (-1)^{(p-1)/2}\left(\frac{p}{3}\right).$$

To determine $\left(\frac{p}{3}\right)$ we need to know the value of $p \bmod 3$. To determine $(-1)^{(p-1)/2}$ we need to know the value of $(p-1)/2 \bmod 2$, or equivalently, the value of $p \bmod 4$. Thus there are only four cases to consider, $p \equiv 1, 5, 7$ or $11 \bmod 12$. Note that the other cases are excluded because $\varphi(12) = 4$ and p must be coprime to 12 (since $p \geq 5$).

Case (i): $p \equiv 1 \bmod 12$. In this case $p \equiv 1 \bmod 3$ so $\left(\frac{p}{3}\right) = 1$.
Also $p \equiv 1 \bmod 4$ so $(p-1)/2$ is even. Hence $\left(\frac{3}{p}\right) = 1$.

Case (ii): $p \equiv 5 \bmod 12$. In this case $p \equiv 2 \bmod 3$ so

$$\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{(3^2-1)/8} = -1.$$

Also $p \equiv 1 \bmod 4$ so $(p-1)/2$ is even. Hence $\left(\frac{3}{p}\right) = -1$.

Case (iii): $p \equiv 7 \bmod 12$. In this case $p \equiv 1 \bmod 3$ so $\left(\frac{p}{3}\right) = 1$.
Also $p \equiv 3 \bmod 4$ so $(p-1)/2$ is odd. Hence $\left(\frac{3}{p}\right) = -1$.

Case (iv): $p \equiv 11 \bmod 12$. In this case $p \equiv 2 \bmod 3$ so $\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$.
Also $p \equiv 3 \bmod 4$ so $(p-1)/2$ is odd. Hence $\left(\frac{3}{p}\right) = 1$.

Summarising our results, we have

$$\left(\frac{3}{p}\right) = \begin{cases} +1, & \text{if } p \equiv \pm 1 \bmod 12, \\ -1, & \text{if } p \equiv \pm 5 \bmod 12. \end{cases}$$

3.6 The Jacobi Symbol

Definition 3.27. Let n be an odd positive integer with prime factorisation $n = p_1^{e_1} \cdots p_r^{e_r}$. Then for any $a \in \mathbb{Z}$ we define the Jacobi symbol $\left(\frac{a}{n}\right)$ by

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{e_i},$$

where the symbols on the right are Legendre symbols. We also define $\left(\frac{a}{1}\right) = 1$.

Theorem 3.28. *Let n be an odd positive integer and let $a \in \mathbb{Z}$.*

(i) $\left(\frac{a}{n}\right) = \pm 1$ *if a and n are coprime and* $\left(\frac{a}{n}\right) = 0$ *otherwise,*
(ii) $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$ *whenever* $a \equiv b \bmod n$*,*
(iii) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ *and* $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$*,*
(iv) $\left(\frac{a^2}{n}\right) = 1$ *whenever a and n are coprime.*

Proof. These properties are easily deduced from the corresponding properties of the Legendre Symbol. □

Remark 3.29. Let n be an odd positive integer with prime factorisation $n = p_1^{e_1} \cdots p_r^{e_r}$. If the congruence

$$x^2 \equiv a \bmod n$$

has a solution then $\left(\frac{a}{p_i}\right) = 1$ for each i and hence $\left(\frac{a}{n}\right) = 1$. However, the converse is not true since because an even number of factors -1 could appear in the defining product of $\left(\frac{a}{n}\right)$. This is illustrated in the following example.

Example 3.30. We have

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1.$$

Even though $\left(\frac{2}{15}\right) = 1$ the congruence $x^2 \equiv 2 \bmod 15$ is insoluble because $x^2 \equiv 2 \bmod 3$ has no solutions.

Theorem 3.31. *If n is an odd positive integer then* $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.

Proof. Write $n = p_1 p_2 \cdots p_r$ where the odd prime factors p_i are not necessarily distinct. Then we have

$$n = \prod_{i=1}^{r}(1 + p_i - 1) = 1 + \sum_{i=1}^{r}(p_i - 1) + \sum_{i \neq j}(p_i - 1)(p_j - 1) + \cdots .$$

But each factor $p_i - 1$ is even so each sum after the first is divisible by 4. Hence

$$n \equiv 1 + \sum_{i=1}^{r}(p_i - 1) \bmod 4,$$

which gives

$$\frac{1}{2}(n-1) \equiv \sum_{i=1}^{r}\frac{1}{2}(p_i - 1) \bmod 2.$$

Therefore

$$\left(\frac{-1}{n}\right) = \prod_{i=1}^{r}\left(\frac{-1}{p_i}\right) = \prod_{i=1}^{r}(-1)^{(p_i-1)/2} = (-1)^{\sum_{i=1}^{r}(p_i-1)/2} = (-1)^{(n-1)/2},$$

which gives the desired result. □

Theorem 3.32. *If n is an odd positive integer then*

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8} = \begin{cases} +1, & n \equiv \pm 1 \bmod 8, \\ -1, & n \equiv \pm 3 \bmod 8. \end{cases}$$

Proof. Write $n = p_1 p_2 \cdots p_r$ where the odd prime factors p_i are not necessarily distinct. Then we have

$$n^2 = \prod_{i=1}^{r}(1 + p_i^2 - 1) = 1 + \sum_{i=1}^{r}(p_i^2 - 1) + \sum_{i \neq j}(p_i^2 - 1)(p_j^2 - 1) + \cdots .$$

Since each p_i is odd, we have $p_i^2 - 1 \equiv 0 \bmod 8$ so

$$n^2 \equiv 1 + \sum_{i=1}^{r}(p_i^2 - 1) \bmod 64$$

hence

$$\frac{1}{8}(n^2 - 1) \equiv \sum_{i=1}^{r}\frac{1}{8}(p_i^2 - 1) \bmod 8.$$

This also holds modulo 2, hence

$$\left(\frac{2}{n}\right) = \prod_{i=1}^{r} \left(\frac{2}{p_i}\right) = \prod_{i=1}^{r} (-1)^{(p_i^2-1)/8} = (-1)^{(n^2-1)/8}.$$

As n is odd we must have $n \equiv \pm 1, \pm 3 \bmod 8$ and by checking the cases $n = \pm 1, \pm 3$ we deduce that

$$\frac{n^2-1}{8} \equiv \begin{cases} 0 \bmod 2, & n \equiv \pm 1 \bmod 8, \\ 1 \bmod 2, & n \equiv \pm 3 \bmod 8. \end{cases}$$

This completes the proof. □

Theorem 3.33 (Reciprocity Law for Jacobi symbols)**.** *Let m and n be coprime odd positive integers. Then*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{(m-1)(n-1)/4} = \begin{cases} +1 & \textit{if } m \equiv 1 \bmod 4 \ \textit{ or } \ n \equiv 1 \bmod 4, \\ -1, & \textit{if } m \equiv n \equiv 3 \bmod 4. \end{cases}$$

Proof. Write $n = p_1 p_2 \cdots p_r$ where the odd prime factors p_i are not necessarily distinct. Similarly, write $m = q_1 q_2 \cdots q_s$ where the odd prime factors q_j are not necessarily distinct. (Note that since m and n are coprime, we have $p_i \neq q_j$ for all i, j.) Then

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s} \left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = (-1)^t$$

for some $t \in \mathbb{Z}$. Applying the quadratic reciprocity law (Theorem 3.23) to the first factor of each term $\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)$, we see that we can take

$$t = \sum_{i=1}^{r}\sum_{j=1}^{s} \frac{1}{2}(p_i - 1)\frac{1}{2}(q_j - 1) = \sum_{i=1}^{r} \frac{1}{2}(p_i - 1) \sum_{j=1}^{s} \frac{1}{2}(q_j - 1).$$

However, the same argument as in the proof of Theorem 3.31 shows that

$$\frac{1}{2}(n-1) \equiv \sum_{i=1}^{r} \frac{1}{2}(p_i - 1) \bmod 2$$

and the corresponding result holds for $\frac{1}{2}(m-1)$. Therefore

$$t \equiv \frac{n-1}{2}\frac{m-1}{2} \bmod 2,$$

which completes the proof. □

Example 3.34. Determine whether 888 is a quadratic residue or nonresidue of the prime 1999. We have

$$\left(\frac{888}{1999}\right) = \left(\frac{2}{1999}\right)^3 \left(\frac{111}{1999}\right) = \left(\frac{111}{1999}\right)$$

since $1999 \equiv -1 \bmod 8$. To calculate $\left(\frac{111}{1999}\right)$ using Legendre symbols, we would write

$$\left(\frac{111}{1999}\right) = \left(\frac{3}{1999}\right)\left(\frac{37}{1999}\right)$$

and apply the quadratic reciprocity law to each factor on the right. However, the calculation is much simpler with the Jacobi symbol since we have

$$\left(\frac{111}{1999}\right) = -\left(\frac{1999}{111}\right) = -\left(\frac{1}{111}\right) = -1$$

since $111 \equiv 1999 \equiv 3 \bmod 4$ and $1999 \equiv 1 \bmod 111$. Therefore 888 is a quadratic nonresidue of 1999.

Example 3.35. Determine whether -104 is a quadratic residue or nonresidue of the prime 997. Since $104 = 2^3 \times 13$ we have

$$\begin{aligned}\left(\frac{-104}{997}\right) &= \left(\frac{-1}{997}\right)\left(\frac{2}{997}\right)^3\left(\frac{13}{997}\right)\\ &= \left(\frac{2}{997}\right)^3\left(\frac{13}{997}\right) \quad \text{since } 997 \equiv 1 \bmod 4\\ &= -\left(\frac{13}{997}\right) \quad \text{since } 997 \equiv -3 \bmod 8\\ &= -\left(\frac{997}{13}\right) \quad \text{since } 997 \equiv 1 \bmod 4\\ &= -\left(\frac{9}{13}\right) \quad \text{since } 997 \equiv 9 \bmod 13\\ &= -1 \quad \text{since 9 is a square.}\end{aligned}$$

Therefore -104 is a quadratic nonresidue of 997.

4 Sums of Squares

4.1 Pythagorean triples

Definition 4.1. A Pythagorean triple (x, y, z) is a triple of positive integers satisfying

$$x^2 + y^2 = z^2.$$

If $\gcd(x, y, z) = 1$ then (x, y, z) is called a primitive Pythagorean triple.

Remark 4.2. If $g = \gcd(x, y, z)$ then $(x/g, y/g, z/g)$ is also a Pythagorean triple. It follows that if $g > 1$, (x, y, z) can be obtained from the "smaller" primitive Pythagorean triple $(x/g, y/g, z/g)$ by multiplying each entry by g. Thus it is natural to focus on primitive Pythagorean triples.

It will be useful to note a basic fact about primitive Pythagorean triples.

Theorem 4.3. *Let (x, y, z) be a primitive Pythagorean triple. Then* $\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1$.

Proof. Suppose $\gcd(x, y) > 1$. Then there is a prime p with $p \mid x$ and $p \mid y$. Then $z^2 = x^2 + y^2 \equiv 0 \pmod{p}$. As $p \mid z^2$ then by Euclid's Lemma for primes we have $p \mid z$ and so $p \mid \gcd(x, y, z)$, contradicting (x, y, z) being a primitive Pythagorean triple. Thus $\gcd(x, y) = 1$.

The proofs that $\gcd(x, z) = 1$ and $\gcd(y, z) = 1$ are similar. □

Considering things modulo 4 we can determine the parities of the numbers in a primitive Pythagorean triple.

Theorem 4.4. *If (x, y, z) is a primitive Pythagorean triple, then one of x and y is even, and the other odd. (Equivalently, $x + y$ is odd.) Also z is odd.*

Proof. Note that if x is even then $x^2 \equiv 0 \pmod{4}$ and if x is odd then $x^2 \equiv 1 \pmod{4}$. If x and y are both odd then $x^2 \equiv y^2 \equiv 1 \pmod{4}$. Hence $z^2 \equiv x^2 + y^2 \equiv 2 \pmod{4}$, which is impossible. If x and y are both even, then $\gcd(x, y) \geq 2$ contradicting Theorem 4.3. We conclude that one of x and y is even, and the other is odd.

In any case, $z \equiv z^2 = x^2 + y^2 \equiv x + y \pmod{2}$, so z is odd. □

As the rôles of x and y in Pythagorean triples are symmetric, it makes little loss in generality in studying only primitive Pythagorean triples with x odd and y even.

We can now prove a theorem characterizing primitive Pythagorean triples

Theorem 4.5. *Let (x, y, z) be a primitive Pythagorean triple with x odd. Then there are r, $s \in \mathbb{N}$ with $r > s$,* $\gcd(r, s) = 1$ *and $r + s$ odd, such that $x = r^2 - s^2$, $y = 2rs$ and $z = r^2 + s^2$.*

Conversely, if r, $s \in \mathbb{N}$ with $r > s$, $\gcd(r, s) = 1$ *and $r + s$ odd, then $(r^2 - s^2, 2rs, r^2 + s^2)$ is a primitive Pythagorean triple.*

Proof. Let (x, y, z) be a primitive Pythagorean triple with x odd. Then y is even and z is odd. Let $a = \frac{1}{2}(z - x)$, $b = \frac{1}{2}(z + x)$ and $c = y/2$. Then a, b, $c \in \mathbb{N}$. Also

$$ab = \frac{(z - x)(z + x)}{4} = \frac{z^2 - x^2}{4} = \frac{y^2}{4} = c^2.$$

Let $g = \gcd(a, b)$. Then $g \mid (a + b)$ and $g \mid (b - a)$; that is $g \mid z$ and $g \mid x$. As $\gcd(x, z) = 1$, by Theorem 4.3, then $g = 1$, that is $\gcd(a, b) = 1$.

Let p be a prime factor of a. Then $p \nmid b$, so $v_p(b) = 0$. Hence

$$v_p(a) = v_p(a) + v_p(b) = v_p(ab) = v_p(c^2) = 2v_p(c)$$

is even. Thus a is a square. Similarly b is a square. Write $a = s^2$ and $b = r^2$ where r, $s \in \mathbb{N}$. Then $\gcd(r, s) \mid a$ and $\gcd(r, s) \mid b$; as a and b are coprime, $\gcd(r, s) = 1$. Now $x = b - a = r^2 - s^2$; therefore $r > s$. Also $z = a + b = r^2 + s^2$. As $c^2 = ab = r^2 s^2$, $c = rs$ and so $y = 2rs$. Finally as x is odd, then $1 \equiv x = b - a \equiv r^2 - s^2 \equiv r^2 + s^2 \equiv r + s \bmod 2$; that is $r + s$ is odd. This proves the first half of the theorem.

To prove the second part, let r, $s \in \mathbb{N}$ with $r > s$, $\gcd(r, s) = 1$ and $r + s$ odd. Set $x = r^2 - s^2$, $y = 2rs$ and $z = r^2 + s^2$. Certainly y, $z \in \mathbb{N}$ and also $x \in \mathbb{N}$ as $r > s > 0$. Also

$$x^2 + y^2 = (r^2 - s^2)^2 + (2rs)^2 = (r^4 - 2r^2 s^2 + s^4) + 4r^2 s^2 = r^4 + 2r^2 s^2 + s^4 = z^2.$$

Hence (x, y, z) is a Pythagorean triple. Certainly y is even, and $x = r^2 - s^2 \equiv r - s \equiv r + s \pmod 2$: x is odd. To show that (x, y, z) is a primitive Pythagorean triple we examine $g = \gcd(x, z)$. Since x is odd, g is odd. Also $g \mid (x + z)$ and $g \mid (z - x)$, that is $g \mid 2r^2$ and $g \mid 2s^2$. As r and s are coprime, then $\gcd(2r^2, 2s^2) = 2$, and so $g \mid 2$. As g is odd $g = 1$. Hence (x, y, z) is a primitive Pythagorean triple. □

We now apply this to the proof of Fermat's last theorem for exponent 4.

Theorem 4.6. *There do not exist x, y, $z \in \mathbb{N}$ with*

$$x^4 + y^4 = z^4. \tag{18}$$

Proof. In fact we prove a stronger result. We claim that there are no x, y, $u \in \mathbb{N}$ with

$$x^4 + y^4 = u^2. \tag{19}$$

A natural number solution (x, y, z) to (18) gives one for (19), namely $(x, y, u) = (x, y, z^2)$. Thus it suffices to prove that (19) is insoluble over $\mathbb{N}$.

We use Fermat's method of descent. Given a solution (x, y, u) of (19) we produce another solution (x', y', u') with $u' < u$. This is a contradiction if we start with the solution of (19) minimizing u.

Let (x, y, u) be a solution of (19) over $\mathbb{N}$ with minimum possible u. We claim first that $\gcd(x, y) = 1$. If not, then $p \mid x$ and $p \mid y$ for some prime p. Then $p^4 \mid (x^4 + y^4)$, that is, $p^4 \mid u^2$. Hence $p^2 \mid u$. Then $(x', y', u') = (x/p, y/p, u/p^2)$ is a solution of (19) in $\mathbb{N}$ with $u' < u$. This is a contradiction. Hence $\gcd(x, y) = 1$.

As $\gcd(x, y) = 1$ then $\gcd(x^2, y^2) = 1$, and so (x^2, y^2, u) is a primitive Pythagorean triple by (19). By the symmetry of x and y we may assume that x^2 is odd and y^2 is even, that is, x is odd and y is even. Hence by Theorem 4.5 there are r, $s \in \mathbb{N}$ with $\gcd(r, s) = 1$

$$x^2 = r^2 - s^2, \quad y^2 = 2rs, \quad u = r^2 + s^2.$$

Then $x^2 + s^2 = r^2$, and as $\gcd(r, s) = 1$ then (x, s, r) is a primitive Pythagorean triple. As x is odd, there exist a, $b \in \mathbb{N}$ with $\gcd(a, b) = 1$ and

$$x = a^2 - b^2, \quad s = 2ab, \quad r = a^2 + b^2$$

by Theorem 4.5. Then

$$y^2 = 2rs = 4(a^2 + b^2)ab,$$

equivalently $(y/2)^2 = ab(a^2 + b^2) = abr$. (Recall that y is even.) If p is prime and $p \mid \gcd(a, r)$ then $b^2 = (a^2 + b^2) - a^2 \equiv 0 \pmod{p}$ and so $p \mid b$ by Euclid's Lemma for primes. This is impossible, as $\gcd(a, b) = 1$. Thus $\gcd(a, r) = 1$. Similarly $\gcd(b, r) = 1$. Now abr is a square. If $p \mid a$, then $p \nmid b$ and $p \nmid r$. Thus $v_p(a) = v_p(abr)$ is even, and so a is a square. Similarly b and r are squares. Write $a = x'^2$, $b = y'^2$ and $r = u'^2$ where x', y', $u' \in \mathbb{N}$. Then

$$u'^2 = a^2 + b^2 = x'^4 + y'^4$$

so (x', y', u') is a solution of (19). Also

$$u' \le u'^2 = a^2 + b^2 = r \le r^2 < r^2 + s^2 = u.$$

This contradicts the minimality of u in the solution (x, y, u) of (19). Hence (19) is insoluble over $\mathbb{N}$. Consequently (18) is insoluble over $\mathbb{N}$. □

4.2 Sums of Squares

Definition 4.7. For $k \in \mathbb{N}$ we let $S_k = \{a_1^2 + \cdots + a_k^2 : a_1, \ldots, a_k \in \mathbb{Z}\}$ be the set of sums of k squares. Note that we allow zero; e.g. $1 = 1^2 + 0^2 \in S_2$.

Theorem 4.8. *The sets S_2 and S_4 are closed under multiplication. That is:*

(i) *If m, $n \in S_2$ then $mn \in S_2$.*

(ii) *If m, $n \in S_4$ then $mn \in S_4$.*

Proof. Let m, $n \in S_2$. Then $m = a^2 + b^2$ and $n = r^2 + s^2$ where a, b, r, $s \in \mathbb{Z}$. By the *two-square* formula,

$$(a^2 + b^2)(r^2 + s^2) = (ar - bs)^2 + (as + br)^2,$$

it is immediate that $mn \in S_2$.

Let m, $n \in S_4$. Then $m = a^2 + b^2 + c^2 + d^2$ and $n = r^2 + s^2 + t^2 + u^2$ where a, b, c, d, r, s, t, $u \in \mathbb{Z}$. By the *four-square* formula,

$$\begin{aligned} & (a^2 + b^2 + c^2 + d^2)(r^2 + s^2 + t^2 + u^2) \\ = \; & (ar - bs - ct - du)^2 + (as + br + cu - dt)^2 \\ & + (at - bu + cr + ds)^2 + (au + bt - cs + dr)^2, \end{aligned}$$

it is immediate that $mn \in S_4$. □

Remark 4.9. The two-square formula comes from complex numbers:

$$\begin{aligned} (a^2 + b^2)(c^2 + d^2) &= |a + bi|^2 |c + di|^2 \\ &= |(a + bi)(c + di)|^2 \\ &= |(ac - bd) + (ad + bc)i|^2 \\ &= (ac - bd)^2 + (ad + bc)^2. \end{aligned}$$

Similarly the four-square formula comes from the theory of quaternions (if you know what they are).

4.3 Sums of Two Squares

We can restrict the possible factorizations of a sum of two squares.

Theorem 4.10. *Let p be a prime with $p \equiv 3 \pmod 4$ and let $n \in \mathbb{N}$. If $n \in S_2$ then $v_p(n)$ is even.*

Proof. Let $n = a^2 + b^2$ with a, $b \in \mathbb{Z}$ and suppose $p \mid n$. We aim to show that $p \mid a$ and $p \mid b$. Suppose $p \nmid a$. Then there is $c \in \mathbb{Z}$ with $ac \equiv 1 \pmod p$. Then

$$0 \equiv c^2 n = (ac)^2 + (bc)^2 \equiv 1 + (bc)^2 \pmod p.$$

This implies that $\left(\frac{-1}{p}\right) = 1$, but we know that $\left(\frac{-1}{p}\right) = -1$ when $p \equiv 3 \pmod 4$. This contradiction proves that $p \mid a$. Similarly $p \mid b$. Thus $p^2 \mid (a^2 + b^2) = n$ and $n/p^2 = (a/p)^2 + (b/p)^2 \in S_2$.

Let $n \in S_2$ and $k = v_p(n)$. We have seen that if $k > 0$ then $k \geq 2$ and $n/p^2 \in S_2$. Note that $v_p(n/p^2) = k - 2$. Similarly if $k - 2 > 0$ (that is if $k > 2$) then $k-2 \geq 2$ (that is $k \geq 4$) and $n/p^4 \in S_2$. Iterating this argument, we find that if $k = 2r + 1$ is odd, then $n/p^{2r} \in S_2$ and $v_p(n/p^{2r}) = 1$, which is impossible. We conclude that k is even. □

Remark 4.11. If $n \in \mathbb{N}$, we can write $n = rm^2$ where m^2 is the largest square dividing n and r is *squarefree*, that is either $r = 1$ or r is a product of distinct primes. If any prime factor p of r is congruent to 3 modulo 4 then $v_p(n) = 1 + 2v_p(m)$ is odd, and $n \notin S_2$. Hence, if $n \in S_2$, the only possible prime factors of r are $p = 2$ and the p congruent to 1 modulo 4. Obviously $2 = 1^2 + 1^2 \in S_2$. It would be nice if all primes congruent to 1 modulo 4 were also in S_2. Fortunately, this is the case.

Theorem 4.12. *Let p be a prime with $p \equiv 1 \pmod 4$. Then $p \in S_2$.*

Proof. As $p \equiv 1 \pmod 4$ then $\left(\frac{-1}{p}\right) = 1$ and so there exists $u \in \mathbb{Z}$ such that $u^2 \equiv -1 \pmod p$. Let

$$\begin{aligned} A &= \{(m_1, m_2) : m_1, m_2 \in \mathbb{Z},\ 0 \leq m_1, m_2 < \sqrt{p}\} \\ &= \{(m_1, m_2) : m_1, m_2 \in \mathbb{Z},\ 0 \leq m_1, m_2 \leq \lfloor \sqrt{p} \rfloor\}. \end{aligned}$$

Then A has $(1 + \lfloor \sqrt{p} \rfloor)^2$ elements and so $|A| > p$.

For $\mathbf{m} = (m_1, m_2) \in \mathbb{R}^2$ define $\phi(\mathbf{m}) = um_1 + m_2$. Then $\phi : \mathbb{R}^2 \longrightarrow \mathbb{R}$ is a linear map, and if $\mathbf{m} \in \mathbb{Z}^2$ then $\phi(\mathbf{m}) \in \mathbb{Z}$.

As $|A| > p$, the $\phi(\mathbf{m})$ for $\mathbf{m} \in A$ can't all be distinct modulo p. Hence there are distinct $\mathbf{m}$, $\mathbf{n} \in A$ with $\phi(\mathbf{m}) \equiv \phi(\mathbf{n}) \pmod p$. Let $\mathbf{a} = \mathbf{m} - \mathbf{n}$. Then by linearity $\phi(\mathbf{a}) = \phi(\mathbf{m}) - \phi(\mathbf{n}) \equiv 0 \pmod p$. Write $\mathbf{a} = (a, b)$. Then $a = m_1 - n_1$ where $0 \leq m_1, n_1 < \sqrt{p}$ so that $|a| < \sqrt{p}$. Similarly $|b| < \sqrt{p}$. Then $a^2 + b^2 < 2p$. As $\mathbf{m} \neq \mathbf{n}$ then $\mathbf{a} \neq (0, 0)$ and so $a^2 + b^2 > 0$. But $0 \equiv \phi(\mathbf{a}) = ua + b \pmod p$. Hence $b \equiv -ua \pmod p$ and so

$$a^2 + b^2 \equiv a^2 + (-ua)^2 \equiv a^2(1 + u^2) \equiv 0 \pmod p$$

As $a^2 + b^2$ is a multiple of p, and $0 < a^2 + b^2 < 2p$, then $a^2 + b^2 = p$. We conclude that $p \in S_2$. □

Alternative proof (constructive). As $p \equiv 1 \pmod 4$ then $\left(\frac{-1}{p}\right) = 1$ and so there exists $u \in \mathbb{Z}$ such that $u^2 \equiv -1 \pmod p$. In other words, there exists $m \in \mathbb{N}$ such that $u^2 + 1 = mp$. Note that we can assume $|u| < \frac{p}{2}$, so $u^2 + 1 < \frac{p^2}{4} + 1 < \frac{p^2}{2}$. Thus $1 \leq m < \frac{p}{2}$.

The idea is as follows. Given a representation $a^2 + b^2 = mp$, with $1 \leq m < p$, use this to find another representation $c^2 + d^2 = m'p$ with $1 \leq m' < m$. Then repeat this process until it terminates (as it must) with $m' = 1$, giving the desired solution. Note that the starting point is the representation $u^2 + 1^2 = mp$ of the first paragraph.

So suppose that $a^2 + b^2 = mp$ for some $m \in \mathbb{N}$ with $1 < m < p$. (If $m = 1$ then we are already done.) Then there exist $a', b' \in \mathbb{Z}$ with $a \equiv a' \bmod m$, $|a'| \leq \frac{m}{2}$ and $b \equiv b' \bmod m$, $|b'| \leq \frac{m}{2}$. Let $c = \frac{aa'+bb'}{m}$ and $d = \frac{ab'-ba'}{m}$. Now

$$aa' + bb' \equiv a^2 + b^2 \equiv 0 \bmod m \quad \text{and} \quad ab' - ba' \equiv ab - ba \equiv 0 \bmod m,$$

and so $c, d \in \mathbb{Z}$. Moreover, $(a')^2 + (b')^2 \equiv a^2 + b^2 \equiv 0 \bmod m$ and so

$$c^2 + d^2 = \frac{(aa' + bb')^2 + (ab' - ba')^2}{m^2} = \frac{(a^2 + b^2)(a'^2 + b'^2)}{m^2} = \frac{p(a'^2 + b'^2)}{m}$$

is in fact an integer and a multiple of p. In other words, $c^2 + d^2 = m'p$ for some $m' \in \mathbb{Z}$. Now $a'^2 \leq \frac{m^2}{4}$ and $b'^2 \leq \frac{m^2}{4}$, so $a'^2 + b'^2 \leq \frac{m^2}{2}$. Thus

$$0 \leq m' = \frac{a'^2 + b'^2}{m} \leq \frac{m}{2} < m < p.$$

If $m' = 0$ then $a' = b' = 0$. Thus $m \mid a$ and $m \mid b$ and so $m^2 \mid (a^2 + b^2) = mp$. Thus $m \mid p$. But p is prime and $1 < m < p$, so $m \nmid p$ - contradiction. Therefore $1 \leq m' < m$. □

Remark 4.13. In order to make this into an algorithm for finding an expression $p = a^b + b^2$ when p is a prime with $p \equiv 1 \bmod 4$, we need to solve the equation $u^2 \equiv -1 \bmod p$. (This is the hard part.) Write $p = 4k + 1$ where $k \in \mathbb{N}$. Let g be a primitive root mod p. Then $\mathrm{ord}_p(g) = \varphi(p) = p - 1 = 4k$ and $g^0, g^1, g^2, \ldots, g^{4k-1}$ are congruent to $1, 2, \ldots, p-1$ in some order. Now $x = g^{2k}$ is a solution to $x^2 \equiv 1 \bmod p$ and $x \not\equiv 1 \bmod p$, so $g^{2k} \equiv -1 \bmod p$ by Corollary 2.71. If $t \equiv g^r \bmod p$ where r is odd then t^k is a solution of $x^2 \equiv -1 \pmod p$ since $2kr \equiv 2k \bmod 4k$ (note that $4k = \mathrm{ord}_p(g)$ and use Proposition 2.53). Thus if we pick $t \in \{1, \ldots, p-1\}$ at random, there is a 50% chance that $t \equiv g^r \bmod p$ with r odd. Given such an t, we set $u = t^k$.

Example 4.14. Let $p = 1997$. Note that p is prime and $p \equiv 1 \bmod 4$. Writing $p = 4k + 1$ we have $k = (p-1)/4 = (1997-1)/4 = 499$. Try $t = 2$. Then $2^{499} \equiv 1585 \equiv -412 \bmod 1997$ (one can use the binary powering algorithm to do this). Note that we chose -412 instead of 1585 because $|-412| = 412 < 1997/2$. Check that $(-412)^2 \equiv -1 \bmod 1997$. Set $a = 412$ and $b = 1$. Then $a^2 + b^2 = 169745 = 85 \times 1997$, so $m = 85$.

Now $412 \equiv -13 \bmod 85$. So take $a' = -13$ and $b' = 1$. Set

$$\begin{aligned} c &= \frac{aa' + bb'}{m} = \frac{412 \times (-13) + 1 \times 1}{85} = -63 \\ d &= \frac{ab' - ba'}{m} = \frac{412 \times 1 - 1 \times (-13)}{85} = 5. \end{aligned}$$

Now we have $63^2 + 5^2 = 3994 = 2 \times 1997$. Now let $a = 63$, $b = 5$ and $m = 2$. Then $63 \equiv 1 \bmod 2$ and $5 \equiv 1 \bmod 2$. So we take $a' = b' = 1$ and

$$\begin{aligned} c &= \frac{aa' + bb'}{m} = \frac{63 \times 1 + 5 \times 1}{2} = 34 \\ d &= \frac{ab' - ba'}{m} = \frac{63 \times 1 - 5 \times 1}{2} = 29. \end{aligned}$$

Now we have $34^2 + 29^2 = 1997$, so we are done.

Remark 4.15. In the above example, we need to compute $2^{499} \bmod 1997$ efficiently. The way to do this is to use the binary powering algorithm that was introduced in §2.9.

We now give the computation of $2^{499} \bmod 1997$ (note that in Example 2.67 we worked mod 997 rather than 1997). First we find the binary expansion of 499 as follows:

$$\begin{aligned} 499 &= 2^8 + 243 \\ &= 2^8 + 2^7 + 115 \\ &= 2^8 + 2^7 + 2^6 + 51 \\ &= 2^8 + 2^7 + 2^6 + 2^5 + 19 \\ &= 2^8 + 2^7 + 2^6 + 2^5 + 2^4 + 3 \\ &= 2^8 + 2^7 + 2^6 + 2^5 + 2^4 + 2^1 + 2^0. \end{aligned}$$

So the binary expansion of 499 is 111110011. (This part is exactly the same as in Example 2.67). Now by squaring the previous term each time, we have

$$\begin{aligned} &2^{2^1} \equiv 4 \pmod{1997} \\ &2^{2^2} \equiv 4^2 \equiv 16 \pmod{1997} \\ &2^{2^3} \equiv 16^2 \equiv 256 \pmod{1997} \\ &2^{2^4} \equiv 256^2 \equiv 65536 \equiv 1632 \equiv -365 \pmod{1997} \\ &2^{2^5} \equiv (-365)^2 \equiv 2663424 \equiv 1423 \equiv -574 \pmod{1997} \\ &2^{2^6} \equiv (-574)^2 \equiv 329476 \equiv 1968 \equiv -29 \pmod{1997} \\ &2^{2^7} \equiv (-29)^2 \equiv 841 \pmod{1997} \\ &2^{2^8} \equiv 841^2 \equiv 707281 \equiv 343 \pmod{1997}. \end{aligned}$$

Therefore

$$\begin{aligned} 2^{499} &\equiv 2^{2^0} \times 2^{2^1} \times 2^{2^4} \times 2^{2^5} \times 2^{2^6} \times 2^{2^7} \times 2^{2^8} \pmod{1997} \\ &\equiv 2 \times 4 \times (-365) \times (-574) \times (-29) \times 841 \times 343 \pmod{1997} \\ &\equiv (-2920) \times 16646 \times 288463 \pmod{1997} \\ &\equiv 1074 \times 670 \times 895 \pmod{1997} \\ &\equiv 719580 \times 670 \times 895 \pmod{1997} \\ &\equiv 660 \times 895 \pmod{1997} \\ &\equiv 1585 \pmod{1997}. \end{aligned}$$

We can now characterize the elements of S_2.

Theorem 4.16 (Two-square theorem)**.** *Let $n \in \mathbb{N}$. Then $n \in S_2$ if and only if $v_p(n)$ is even whenever p is a prime congruent to 3 modulo 4.*

Proof. If $n \in S_2$, p is prime and $p \equiv 3 \pmod 4$ then $v_p(n)$ is even by Theorem 4.10.

If $v_p(n)$ is even whenever p is a prime congruent to 3 modulo 4 then $n = rm^2$ where each prime factor p of r is either 2 or congruent to 1 modulo 4. By Theorem 4.12 all primes p with $p \equiv 1 \bmod 4$ lie in S_2. Moreover, $2 = 1^2 + 1^2 \in S_2$. Hence by Theorem 4.8 $r \in S_2$. Hence $r = a^2 + b^2$ where a, $b \in \mathbb{Z}$ and so $n = rm^2 = (am)^2 + (bm)^2 \in S_2$. □

The representation of a prime as a sum of two squares is essentially unique.

Theorem 4.17. *Let p be a prime. If $p = a^2 + b^2 = c^2 + d^2$ with a, b, c, $d \in \mathbb{N}$ then either $a = c$ and $b = d$ or $a = d$ and $b = c$.*

Proof. Consider

$$\begin{aligned} (ac + bd)(ad + bc) &= a^2cd + abc^2 + abd^2 + b^2cd \\ &= (a^2 + b^2)cd + ab(c^2 + d^2) \\ &= pcd + pab \\ &= p(ab + cd). \end{aligned}$$

As $p \mid (ac+bd)(ad+bc)$ then by Euclid's lemma for primes either $p \mid (ac+bd)$ or $p \mid (ad + bc)$. Assume the former — the latter case can be treated by reversing the rôles of c and d. Now $ac + bd > 0$ so that $ac + bd \geq p$. Also

$$\begin{aligned} (ac + bd)^2 + (ad - bc)^2 &= a^2c^2 + 2abcd + b^2d^2 + a^2d^2 - 2abcd + b^2c^2 \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= p^2. \end{aligned}$$

As $ac+bd \geq p$, the only way this is possible is if $ac+bd = p$ and $ad-bc = 0$. Then $ac^2+bcd = cp$ and $ad^2-bcd = 0$, so adding gives $a(c^2+d^2) = cp$, that is $ap = cp$, so that $a = c$. Then $c^2+bd = p = c^2+d^2$ so that $bd = d^2$, so that $b = d$. □

Example 4.18. Find two "essentially different" ways of writing $629 = 17 \times 37$ as the sum of two squares. First note that 17 and 37 are both primes congruent to 1 mod 4, and thus each can be written as the sum of two squares in a unique way. In fact, $17 = 4^2+1^2$ and $37 = 6^2+1^2$. Then

$$\begin{aligned}629 &= |4+i|^2|6+i|^2 = |(4+i)(6+i))|^2 = |23+10i|^2 = 23^2+10^2\\ 629 &= |4+i|^2|6-i|^2 = |(4+i)(6-i))|^2 = |25+2i|^2 = 25^2+2^2.\end{aligned}$$

4.4 Sums of Four Squares

We wish to prove the theorem of Lagrange to the effect that all natural numbers are sums of four squares. It is crucial to establish this for primes.

Theorem 4.19. *Let p be a prime. Then $p \in S_4$.*

Proof. If $p \equiv 1 \pmod 4$ then there are a, $b \in \mathbb{Z}$ with $p = a^2+b^2+0^2+0^2$ (Theorem 4.12) so that $p \in S_4$. Also $2 = 1^2+1^2+0^2+0^2 \in S_4$ and $3 = 1^2+1^2+1^2+0^2 \in S_4$. We may assume that $p > 3$ and that $p \equiv 3 \pmod 4$. As a consequence $\left(\frac{-1}{p}\right) = -1$.

Let w be the smallest positive integer with $\left(\frac{w}{p}\right) = -1$. (Note that this forces $w \geq 2$.) Then

$$\left(\frac{w-1}{p}\right) = 1 \quad \text{and} \quad \left(\frac{-w}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{w}{p}\right) = 1.$$

Hence there are u, $v \in \mathbb{Z}$ with $w-1 \equiv u^2 \pmod p$ and $-w \equiv v^2 \pmod p$. Then $1+u^2+v^2 \equiv 1+(w-1)-w \equiv 0 \pmod p$.

Let

$$\begin{aligned}B &= \{(m_1,m_2,m_3,m_4) : m_1,\ldots,m_4 \in \mathbb{Z}, 0 \leq m_1,\ldots,m_4 < \sqrt{p}\}\\ &= \{(m_1,m_2,m_3,m_4) : m_1,\ldots,m_4 \in \mathbb{Z}, 0 \leq m_1,\ldots,m_4 < \lfloor\sqrt{p}\rfloor\}.\end{aligned}$$

Then B has $(1+\lfloor\sqrt{p}\rfloor)^4$ elements. Hence $|B| > p^2$. For $\mathbf{m} = (m_1,m_2,m_3,m_4)$ define $\psi(\mathbf{m}) = (um_1+vm_2+m_3, -vm_1+um_2+m_4)$. Then $\psi : \mathbb{R}^4 \longrightarrow \mathbb{R}^2$ is a linear map. If $\mathbf{m} \in \mathbb{Z}^4$ then $\psi(\mathbf{m}) \in \mathbb{Z}^2$. We write $(a,b) \equiv (a',b') \pmod p$ if $a \equiv a' \pmod p$ and $b \equiv b' \pmod p$. If we have a list $(a_1,b_1),\ldots,(a_N,b_N)$ of vectors in $\mathbb{Z}^2$ with $N > p^2$, then there must be some distinct i and j with

$(a_i, b_i) \equiv (a_j, b_j) \pmod p$. This happens for the vectors $\psi(\mathbf{m})$ with $\mathbf{m} \in B$ as $|B| > p^2$. Thus there are distinct $\mathbf{m}$, $\mathbf{n} \in B$ with $\psi(\mathbf{m}) \equiv \psi(\mathbf{n}) \pmod p$. Let $\mathbf{a} = \mathbf{m} - \mathbf{n}$. Then $\psi(\mathbf{a}) = \psi(\mathbf{m}) - \psi(\mathbf{n}) \equiv (0,0) \pmod p$. Let $\mathbf{a} = (a,b,c,d)$. Then $a = m_1 - n_1$ where $0 \le m_1, n_1 < \sqrt{p}$ so that $|a| < \sqrt{p}$. Similarly $|b|$, $|c|$, $|d| < \sqrt{p}$. Then $a^2 + b^2 + c^2 + d^2 < 4p$. As $\mathbf{m} \ne \mathbf{n}$ then $\mathbf{a} \ne (0,0,0,0)$ and so $a^2 + b^2 + c^2 + d^2 > 0$.

Now $(0,0) \equiv \psi(\mathbf{a}) = (ua + vb + c, -va + ub + d) \pmod p$. Hence $c \equiv -ua - vb \pmod p$ and $d \equiv va - ub \pmod p$. Then

$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &\equiv a^2 + b^2 + (ua + vb)^2 + (va - ub)^2 \\ &= (1 + u^2 + v^2)(a^2 + b^2) \equiv 0 \pmod p \end{aligned}$$

where the last equality holds because we previously showed that $1 + u^2 + v^2 \equiv 0 \bmod p$. As $a^2 + b^2 + c^2 + d^2$ is a multiple of p, and $0 < a^2 + b^2 + c^2 + d^2 < 4p$, then we must have $a^2 + b^2 + c^2 + d^2 \in \{p, 2p, 3p\}$.

When $a^2 + b^2 + c^2 + d^2 = p$ then certainly $p \in S_4$. Alas, we need to consider the bothersome cases where $a^2 + b^2 + c^2 + d^2 = 2p$ or $3p$.

Suppose that $a^2 + b^2 + c^2 + d^2 = 2p$. Then $a^2 + b^2 + c^2 + d^2 \equiv 2 \pmod 4$ so that two of a, b, c, d are odd and the other two even. Without loss of generality a and b are odd and c and d are even. Then $\frac{1}{2}(a+b)$, $\frac{1}{2}(a-b)$, $\frac{1}{2}(c+d)$ and $\frac{1}{2}(c-d)$ are all integers, and a simple computation gives

$$\left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 = \frac{a^2 + b^2 + c^2 + d^2}{2} = p$$

so that $p \in S_4$.

Finally suppose that $a^2 + b^2 + c^2 + d^2 = 3p$. Then $a^2 + b^2 + c^2 + d^2$ is a multiple of 3 but not 9. As $a^2 \equiv 0$ or $1 \pmod 3$ then either exactly one or all four of a, b, c and d are multiples of 3. But the latter case is impossible (for then $a^2 + b^2 + c^2 + d^2$ would be a multiple of 9), so without loss of generality $3 \mid a$ and b, c, $d \equiv \pm 1 \pmod 3$. By replacing b by $-b$ etc., if necessary, we may assume that $b \equiv c \equiv d \equiv 1 \pmod 3$. Then $\frac{1}{3}(b + c + d)$, $\frac{1}{3}(a + b - c)$, $\frac{1}{3}(a + c - d)$,$\frac{1}{3}(a + d - b)$, are all integers, and a simple computation gives

$$\begin{aligned} &\left(\frac{b+c+d}{3}\right)^2 + \left(\frac{a+b-c}{3}\right)^2 + \left(\frac{a+c-d}{3}\right)^2 + \left(\frac{a+d-b}{3}\right)^2 \\ = \quad &\frac{a^2 + b^2 + c^2 + d^2}{3} = p \end{aligned}$$

so that $p \in S_4$. □

We can now prove Lagrange's four-square theorem.

Theorem 4.20 (Lagrange)**.** *If* $n \in \mathbb{N}$ *then* $n \in S_4$*.*

Proof. Either $n = 1 = 1^2 + 0^2 + 0^2 + 0^2 \in S_4$, or n is a product of a sequence of primes. By Theorem 4.19, each prime factor of n lies in S_4. Then since S_4 is closed under multiplication (Theorem 4.8), we have $n \in S_4$. □