ECM3704 NUMBER THEORY

EXERCISE SHEET 1 – SOLUTIONS

This sheet does not count for assessment

1. The primes up to 200 are:

2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97,101,103,
107,109,113,127,131,137,139,149,151,157,163,167,173,179,181,191,193,197,199.

2. (i)

i	r_{i-2}		r_{i-1}		q_{i-1}		r_i	x_i	y_i
0							34	1	0
1							20	0	1
2	34	$=$	20	$\times$	1	$+$	14	1	-1
3	30	$=$	14	$\times$	1	$+$	6	-1	2
4	14	$=$	6	$\times$	2	$+$	2	3	-5
5	6	$=$	2	$\times$	3	$+$	0		

so $\gcd(34, 20) = 2 = 3 \times 34 - 5 \times 20$ and $x = 3$, $y = -5$.

(ii)

i	r_{i-2}		r_{i-1}		q_{i-1}		r_i	x_i	y_i
0							55	1	0
1							34	0	1
2	55	$=$	34	$\times$	1	$+$	21	1	-1
3	34	$=$	21	$\times$	1	$+$	13	-1	2
4	21	$=$	13	$\times$	1	$+$	8	2	-3
5	13	$=$	8	$\times$	1	$+$	5	-3	5
6	8	$=$	5	$\times$	1	$+$	3	5	-8
7	5	$=$	3	$\times$	1	$+$	2	-8	13
8	3	$=$	2	$\times$	1	$+$	1	13	-21
9	2	$=$	2	$\times$	1	$+$	0		

so $\gcd(55, 34) = 1 = 13 \times 55 - 21 \times 34$ and so $x = 13$, $y = -21$.

(iii)

i	r_{i-2}		r_{i-1}		q_{i-1}		r_i	x_i	y_i
0							1105	1	0
1							208	0	1
2	1105	$=$	208	$\times$	5	$+$	65	1	-5
3	208	$=$	65	$\times$	3	$+$	13	-3	16
4	65	$=$	13	$\times$	5	$+$	0		

so $\gcd(1105, 208) = 13 = -3 \times 1105 + 16 \times 208$ and so $x = -3$, $y = 16$.

3. We have $l = a(b/d)$ with $b/d \in \mathbb{Z}$ so $a \mid l$. Similarly $b \mid l$, so (i) holds.

Let $a' = a/d$, $b' = b/d$. Then a', $b' \in \mathbb{Z}$, $l = a'b'd$ and $\gcd(a', b') = 1$. If $a \mid m$ and $b \mid m$, say $m = ar = bs$, then, dividing by d, we have $a'r = b's$. Thus $a' \mid b's$. By Euclid's Lemma $a' \mid s$. Hence $a'b \mid bs$, that is, $l \mid m$. Thus (ii) holds.

Now suppose that L is another positive integer satisfying (i) and (ii). By (i) for L we have $a \mid L$ and $b \mid L$, so it follows from (ii) for l that $l \mid L$. Similarly $L \mid l$, and as both are positive, we conclude that $L = l$.

4. (i) Suppose that n is an integer such that $n^2 + 2$ is divisible by 4. That is, $4 \mid (n^2 + 2)$, which is to say that

$$n^2 + 2 = 4k$$

for some integer k. Consider two cases:
Case 1: n is even. That is, $n = 2m$ for some integer m. Then we can write $4k = 4m^2 + 2$. Dividing by 2, we have $2k = 2m^2 + 1$. In the last equation we have that the lhs is even and the rhs is odd. This is a contradiction!
Case 2: n is not even. Similar to Case 1. From cases 1 and 2 we have the desired result.

(ii) Note that $x \mid y$ if and only if $(x, y) = x$. We now use some properties of the gcd.

$$\begin{aligned}
a \mid bc &\Leftrightarrow (a, bc) = a \\
&\Leftrightarrow \left(\frac{a}{(a,b)}, \frac{bc}{(a,b)}\right) = \frac{a}{(a,b)} \\
&\Leftrightarrow \left(\frac{a}{(a,b)}, \frac{b}{(a,b)}c\right) = \frac{a}{(a,b)} \\
&\Leftrightarrow \left(\frac{a}{(a,b)}, c\right) = \frac{a}{(a,b)} \qquad\qquad \text{by Euclid's Lemma} \\
&\Leftrightarrow \frac{a}{(a,b)} \mid c.
\end{aligned}$$

5. (i) $60 = 2^2 \cdot 3 \cdot 5$.
$v_2(60) = 2$; $v_3(60) = v_5(60) = 1$;
$v_p(60) = 0$ for all primes $p \neq 2$, 3, 5.

(ii) $105 = 3 \cdot 5 \cdot 7$.
$v_3(105) = v_5(105) = v_7(105) = 1$;
$v_p(105) = 0$ for all primes $p \neq 3$, 5, 7.

(iii) $65536 = 2^{16}$.
$v_2(65536) = 16$; $v_p(65536) = 0$ for all primes $p \neq 2$.

6. It is sufficient to prove the contrapositive, that if $\sqrt{m}$ is rational then m is a perfect square. Suppose that $\sqrt{m} = a/b$ where a and b are positive

integers. Then

$$m = a^2/b^2.$$

If a and b have prime-power factorisations

$$a = p_1^{e_1} \cdots p_k^{e_k} \qquad \text{and} \qquad b = p_1^{f_1} \cdots p_k^{f_k}$$

then

$$m = p_1^{2e_1 - 2f_1} \cdots p_k^{2e_k - 2f_k}$$

must be the factorisation of m. Notice that every prime p_i appears an even number of times in this factorisation, and $e_i - f_i \geq 0$ for each i, so

$$m = \left(p_1^{e_1 - f_1} \cdots p_k^{e_k - f_k}\right)^2$$

is a perfect square.

7. The number k is a proper factor of $(n+1)! + k$ for $2 \leq k \leq n+1$, since k occurs as one of the terms in the product $(n+1)! = (n+1) \cdot n \cdot (n-1) \cdot \ldots \cdot 1$. Hence each of these n numbers $(n+1)! + k$ is composite, so we have exhibited n consecutive composite numbers.

8.
(i) Suppose $p_1, p_2, \ldots, p_n$ are distinct primes of the form $4x - 1$. Consider the number

$$N = 4p_1 p_2 \ldots p_n - 1.$$

Then $p_i \nmid N$ for any i. Moreover, not every prime $p \mid N$ is of the form $4x + 1$; if they all were, then N would be of the form $4x + 1$. Since N is odd, each prime divisor p_i is odd so there is a $p \mid N$ that is of the form $4x - 1$. Since $p \neq p_i$ for any i, we have found a new prime of the form $4x - 1$. We can repeat this process indefinitely, so the set of primes of the form $4x - 1$ cannot be finite.

(ii) Suppose $n = ab$ where $a, b \in \mathbb{N}$ and a is the smallest prime factor of n. Since n is not prime, we have $b > 1$. Since a is the smallest prime factor of n, we have $a \leq b$. Suppose for a contradiction that $a > \sqrt{n}$. Then we also have $b > \sqrt{n}$ and so $n = ab > (\sqrt{n})^2 = n$ - contradiction. Therefore $a \leq \sqrt{n}$.

(iii) If an odd integer n is expressible as a sum of three or more consecutive positive integers, then for some $m \geq 1$ and $k \geq 3$,

$$n = m + (m+1) + \ldots + (m + (k-1)) = km + \frac{k(k-1)}{2}.$$

If k is odd, then $n = k(m + \frac{k-1}{2})$ and cannot be prime (k and $m + \frac{k-1}{2}$ are integers strictly bigger than 1). If k is even, then, $n = \frac{k}{2}(2m + (k-1))$ and once again cannot be prime as $k/2$ and $2m + (k-1)$ are integers strictly bigger than 1. If an odd integer n is not prime, write $n = ab$ for some other positive integers a and b strictly bigger than 1. a and b must be odd. Assume $a \leq b$ without loss of generality. Let $k = a \geq 3$ and $m = b - \frac{a-1}{2} \geq a - \frac{a-1}{2} = \frac{a+1}{2} \geq 2$. Then,

$$m + (m+1) + \cdots + (m + (k-1)) = km + \frac{k(k-1)}{2} = k(m + \frac{k-1}{2}) = ab = n.$$