ECM3704 – NUMBER THEORY

EXERCISE SHEET 2 – OUTLINE SOLUTIONS

1*.

$a^2 \equiv b^2 \pmod p \Leftrightarrow p \mid (a^2-b^2) \Leftrightarrow p \mid (a+b)(a-b) \Leftrightarrow p \mid (a+b)$ or $p \mid (a-b)$.

Where the last part follows from Euclid's Lemma. **[10]**

Total for question: [10]

2.
(i) The second assertion is the special case of the first obtained by using the greatest common divisor g of a and b in the role of d. The first assertion in turn is a direct consequence of Proposition 1.9 (iii) obtained by replacing c, a, b in that proposition by $d, a/d, b/d$ respectively.

(ii) If $ax \equiv ay \pmod m$ then $ay - ax = mz$ for some integer z. Hence we have

$$\frac{a}{(a,m)}(y-x) = \frac{m}{(a,m)}z,$$

and thus

$$\frac{m}{(a,m)} \mid \frac{a}{(a,m)}(y-x).$$

But $(a/(a,m)), m/(a,m)) = 1$ by the result in the first part of the question (i) and therefore $(m/(a,m)) \mid (y-x)$ by Euclid's Lemma. That is,

$$x \equiv y \bmod \left(\frac{m}{(a,m)}\right).$$

Conversely, if $x \equiv y \pmod{(m/(a,m))}$, we multiply by a to get $ax \equiv ay \pmod{(am/(a,m))}$ by use of Proposition 2.10, part (ii). But (a,m) is a divisor of a, so we can write $ax \equiv ay \pmod m$ by Proposition 2.10, part (i).

3. We adapt the proof given in lectures that there are infinitely many primes p with $p \equiv 3 \bmod 4$.

Suppose, for a contradiction, that there are only finitely many primes $p \equiv 2 \pmod 3$. Label them $p_0, p_1, \ldots, p_n$, with $p_0 = 2$. Now consider the number $N = 3 \cdot p_1 \cdot p_2 \cdots p_n + 2$. Notice that N is odd, because it is the product of several odd numbers plus an even number. That means it is not divisible by 2. Also notice that $N \equiv 2 \pmod 3$, so it is not divisible by 3. Finally, notice that no odd prime congruent to 2 mod 3 divides N, since all those primes are included in the product $3 \cdot p_1 \cdot p_2 \cdots p_n$, so if one of those primes were to divide N, it would also divide 2, which is impossible. Now if 3 doesn't divide N, and no prime congruent to 2 mod 3 divides N, then all the prime divisors of N must be 1 mod 3. But this is a contradiction, because then any product of these primes - in particular, N - is 1 mod 3, yet N is 2 mod 3. So we have shown that there are infinitely many primes congruent to 2 mod 3.

4. (i)* $3x \equiv 10 \pmod{13}$
We have $\gcd(3, 13) = 1 = 1 \times 13 - 4 \times 3$ (either using the Extended Euclidean Algorithm, or by inspection). Thus there is a solution, and it is unique mod 13. In fact

$$3 \times (-4) \equiv \quad \pmod{13}, \qquad \text{so } \ 3 \times (-40) \equiv 10 \pmod{13}.$$

Hence solution is $x \equiv -40 \equiv 12 \pmod{13}$. **[4]**

(ii) $12x \equiv 20 \pmod{38}$
Dividing through by 2, we get $6x \equiv 10 \pmod{19}$, and

$$\gcd(6, 19) = 1 = 1 \times 19 - 3 \times 6.$$

Hence solution is $x \equiv -3 \times 10 \equiv 8 \pmod{19}$.

(iii)* $20x \equiv 4 \pmod{30}$
This congruence has no solutions. This is because the left side of the congruence can only be congruent to 0,10 or 20. This is because 20 and 30 share the common factor 10. **[2]**

(iv) $15x \equiv 43 \pmod{99}$
This congruence has no solutions. This is because $\gcd(15, 99) = 3$, which does not divide 43.

(v)* $353x \equiv 254 \pmod{400}$
For this congruence, we can see that x needs to be even. Thus if we let $x = 2y$ then we are solving the reduced congruence $353k \equiv 127 \pmod{200}$. Now to find the inverse of $353 \equiv -47$, we use the Euclidean algorithm and obtain that

$$1 = 200 \times (4) + 47 \times (-17).$$

This shows that 17 is the inverse of $(-47) \pmod{200}$. Thus the solution to the reduced congruence is

$$k \equiv (17)(127) \equiv 2159 \equiv 159 \pmod{200}.$$

Since $x = 2k$, $x = 318$. This solution is unique, mod 400, since $(353, 400) = 1$. **[4]**

Total for question: [10]

5*. (i) $12 \times 13 - 5 \times 31 = 1$, so we get $x \equiv 2 \times 12 \equiv 24 \pmod{31}$. Thus general solution is $x = 24 + 31a$, $y = -10 - 13a$ for arbitrary $a \in \mathbb{Z}$. **[5]**

(ii) $12x + 28y = 16$. Dividing through by 4, we get $3x + 7y = 4$. As $1 \times 7 - 2 \times 3 = 1$, general solution is $x = 7a - 1$, $y = 1 - 3a$ for arbitrary $a \in \mathbb{Z}$. **[5]**

Total for question: [10]

6*. (i) $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, $\phi(6) = 2$, $\phi(7) = 6$, $\phi(8) = 4$, $\phi(9) = 6$, $\phi(10) = 4$, $\phi(11) = 10$, $\phi(12) = 4$. **[3]**

(ii) Since $245 \equiv 11 \pmod{18}$, $245^{1040} \equiv 11^{1040} \pmod{18}$. Since $(11, 18) = 1$, by Euler's theorem, $11^{\phi(18)} \equiv 11^6 \equiv 1 \pmod{18}$. Therefore, $11^{1040} = (11^6)^{173} \times 11^2 \equiv 1^{173} \times 13 \equiv 13 \pmod{18}$. Thus, the desired remainder is 13. **[5]**

(iii) $\phi(1) = 1 = \phi(2)$. $\phi(3) = 2$. For $n = 3$, there are no solutions to $\phi(x) = 3$. For if $3 = \prod_{p \in S}(p^{\alpha_p - p^{\alpha_p - 1}})$ for S some subset of primes and $\alpha_p \geq 1$, then $3 = p^{\alpha-1}(p-1)$ for some prime p (as 3 is prime), so this tell us by unique factorization that either $p^{\alpha-1} = 3$ and $p - 1 = 1$ or $p^{\alpha-1} = 1$ and $p - 1 = 3$. The latter is not possible as 4 is not a prime, and the former is not possible as $2^\alpha \neq 3$ for any α.
For $n = 1$, $\phi(x) = 1$ has exactly two solutions 1 and 2. For if $p > 2$, then $phi(p^\alpha) \geq p - 1 \geq 2$. So if x is a solution to $\phi(x) = 1$, then x cannot have any prime factor other than 2 for if $x = \prod p^\alpha$, $\phi(x) = \prod(\phi(p^\alpha)) \geq \phi(p^\alpha)$. So if at all $\phi(x) = 1$ has to have some other solution other than $x = 1$, then $x = 2^\alpha$ for some α. Again, if $\alpha > 1$, then $\phi(2^\alpha) = 2^{\alpha-1} \geq 2$.
$\phi(x) = 2$ has exactly three solutions 3,4,6. This can be argued again using the fact that 2 is prime. If $x = \prod p^{\alpha_p}$, then no prime strictly bigger than 3 can appear in this product as otherwise, $\phi(x) \geq p - 1 \geq 4$. So we are looking for pairs (α_1, α_2) so that $x = 2^{\alpha_1} 3^{\alpha_2}$ is a solution to $\phi(x) = 2$. As $3 \mid \phi(3^{\alpha_2})$ if $\alpha_2 > 1$ and $3 \nmid 2$, we see that $\alpha_2 \in \{0, 1\}$. If $\alpha_2 = 1$, then α_1 is wither 0 or 1 as then we are looking for solutions to $\phi(2^{\alpha_1}) = 1$. This gives $x = 3$ and $x = 6$. If $\alpha_2 = 0$, then $\phi(2^{\alpha_1}) = 2^{\alpha_1 - 1} = 2$, so $\alpha_1 = 2$. This gives $x = 4$. **[12]**

Total for question: [20]

7*. (i) Here $N = 3 \times 4 \times 5 = 60$, $N_1 = N/3 = 20$, $N_2 = N/4 = 15$, and $N_3 = N/5 = 12$. The unique solutions of the congruences $N_1 y_1 \equiv 1 \pmod{n_1}$, $N_2 y_2 \equiv 1 \pmod{n_2}$, and $N_3 y_3 \equiv 1 \pmod{n_3}$, that is, $20y_1 \equiv 1 \pmod 3$, $15y_2 \equiv 1 \pmod 4$, and $12y_3 \equiv 1 \pmod 5$ are $2, 3$ and 3, respectively. Thus, by the Chinese Remainder Theorem,

$$\begin{aligned} x &\equiv \sum_{i=1}^{3} a_i N_i y_i \pmod N \\ &\equiv 1 \times 20 \times 2 + 2 \times 15 \times 3 + 3 \times 12 \times 3 \pmod{60} \\ &\equiv 58 \pmod{60}. \end{aligned}$$

[5]

(ii) $N_1 = 7$ and $N_2 = 5$. $N_1 y_1 \equiv 1 \pmod{n_1}$ yields $7y_1 \equiv 1 \pmod 5$; that is $y_1 \equiv 3 \pmod 5$. Similarly, $y_2 \equiv 3 \pmod 7$. Thus, $x \equiv \sum_i a_i N_i y_i \equiv 2 \times 7 \times 3 + 3 \times 5 \times 3 \equiv 17 \pmod{35}$. Thus, $x = 17 + 35t$. **[2]**
(iii) Because $x = 2 + 4t$, $2 + 4t \equiv 3 \pmod 6$; that is, $4t \equiv 1 \pmod 6$ which is not solvable because $(4, 6) \neq 1$. **[3]**

Total for question: [10]

8*. $504 = 2^3 \times 3^2 \times 7$. Let the three consecutive numbers be $\{x^3 - 1, x^3, x^3 + 1\}$. Their product is $P = x^3(x^6 - 1)$. $7 \mid x^7 - x$ by Fermat's theorem, and therefore $7 \mid x^2(x^7 - x)$, i.e., $7 \mid P$. $x^6 - 1 = (x^2 - 1)(x^4 + x^2 + 1)$. If $x \equiv 0 \pmod 2$, then $2^3 \mid x^3$ and therefore $8 \mid P$. If $x \not\equiv 0 \pmod 2$, then

$x = 2y+1$ by the division algorithm and $x^2 - 1 = 4y(y+1)$. $2 \mid y^2 - y$ by Fermat's theorem and therefore, $2 \mid (y^2 - y + 2y)$. This shows $8 \mid (x^2 - 1)$ and therefore $8 \mid P$. If $x \equiv 0 \pmod 3$, then $3^2 \mid x^3$ and therefore $3^2 \mid P$. If $x \not\equiv 0 \pmod 3$, then $x^2 \equiv 1 \pmod 3$ which in turn implies $x^4 \equiv 1 \pmod 3$ and therefore $x^4 + x^2 + 1 \equiv 3 \pmod 3 = 0 \pmod 3$. $3 \mid (x^2-1)(x^4+x^2+1)$ and therefore $3^2 \mid P$. As $2^3, 3^2$ and 7 are pairwise coprime, this shows that their product divides P for any x. **[20]**

9*. First we note (by the Chinese Remainder Theorem) that $x \equiv 1 \pmod 7$ and $x \equiv 5 \pmod 7$ are the only solutions of $x^2 + x + 47 \equiv 0 \pmod 7$. Since $f^{'}(x) = 2x+1$, we see that $f^{'}(1) = 3 \not\equiv 0 \pmod 7$ and $f^{'}(5) = 1 \not\equiv 0 \pmod 7$, so these roots are non-singular. Taking $\overline{f^{'}(1)} = 5$ (where $\overline{f^{'}(a)}$ is an integer chosen so that $f^{'}(a)\overline{f^{'}(a)} \equiv 1 \pmod 7$), we see as given in the proof of Hensel's lemma that the root $a \equiv 1 \pmod 7$ lifts to $a_2 = 1 - 49 \times 5$. Since a_2 is considered $\pmod{7^2}$, we may take instead $a_2 = 1$. Then $a_3 = 1 - 49 \times 5 \equiv 99 \pmod{7^3}$. Similarly, we take $\overline{f^{'}(5)} = 2$, and see that the root $5 \pmod 7$ lifts to $5 - 77 \times 2 = -149 \equiv 47 \pmod{7^2}$, and that $47 \pmod{7^2}$ lifts to $47 - f(47) \times 2 = 47 - 2303 \times 2 = -4559 \equiv 243 \pmod{7^3}$. Thus we conclude that 99 and 243 are the desired roots and that there are no others. **[10]**