ECM3704 – NUMBER THEORY

EXERCISE SHEET 3 – OUTLINE SOLUTIONS

1. (i)* $x^2 \equiv -5 \pmod{7^3}$.
First solve mod 7: solutions to $x^2 \equiv -5 \pmod 7$ are $x \equiv \pm 3 \pmod 7$. Try lifting $x = 3$ to a solution mod 7^2: Putting $x = 3 + 7a$ and substituting into $x^2 \equiv -5 \pmod{7^2}$, we find $6 \times 7a \equiv -14 \pmod{7^2}$, so $a \equiv 2 \pmod 7$, and $x \equiv 3 + 2 \times 7 = 17 \pmod{7^2}$. Now lift again to a solution mod 7^3: put $x = 17 + 49a$. We find $6 \times 49a \equiv -294 \pmod{7^3}$ so $a \equiv 6 \equiv -1 \pmod 7$. Hence $x \equiv -32 \pmod{7^3}$.
This shows that the solution $x \equiv 3 \pmod 7$ lifts to $x \equiv -32 \pmod{7^3}$. Since x^2 is an even function, the solution $x \equiv -3 \pmod 7$ must lift to $x \equiv 32 \pmod{7^3}$. Hence solution to $x \equiv -5 \pmod{7^3}$ is $x \equiv \pm 32 \pmod{7^3}$. [**5**]

(ii)* $x^2 \equiv 3 \pmod{7^3}$ has no solutions since there are no solutions to $x^2 \equiv 3 \pmod 7$ (one can compute the Legendre symbol to check this). [**3**]

(iii)* Starting with $x^2 + x + 7 \equiv 0 \pmod 3$, we note that $x = 1$ is the only solution. Here $f'(1) = 3 \equiv 0 \pmod 3$, and $f(1) \equiv 0 \pmod 9$, so that we have roots $x = 1$, $x = 4$, and $x = 7 \pmod 9$. Now $f(1) \not\equiv 0 \pmod{27}$, and hence there is no root $x \pmod{27}$ for which $x \equiv 1 \pmod 9$. As $f(4) \equiv 0 \pmod{27}$, we obtain three roots, 4, 13, 22 $\pmod{27}$, which are $\equiv 4 \pmod 9$. On the other hand, $f(7) \not\equiv 0 \pmod{27}$, so there is no root $\pmod{27}$ that is $\equiv 7 \pmod 9$. We are now in a position to determine which, if any, of the roots 4, 13, 22 $\pmod{27}$ can be lifted to roots $\pmod{81}$. We find that $f(4) = 27 \not\equiv 0 \pmod{81}$, $f(13) = 189 \equiv 27 \not\equiv 0 \pmod{81}$, and that $f(22) = 513 \equiv 27 \not\equiv 0 \pmod{81}$, from which we deduce that the congruence has no solution $\pmod{81}$. [**7**]

(iv) $x^3 + x^2 + 8 \equiv 0 \pmod{11^3}$.
Testing all possibilities mod 11, we find two solutions, $x \equiv 3, 4 \pmod{11}$.
Try lifting $x \equiv 3 \pmod{11}$: set $x = 3+11a$. Substituting into the congruence we get $44 + 11a \times 33 \equiv 0 \pmod{11^2}$ which simplifies to $0a \equiv -4 \pmod{11}$. This has no solutions, so the solution $x \equiv 3 \pmod{11}$ of the given congruence **does not** lift to a solution mod 11^2, and hence does not lift to a solution mod 11^3.
Now try lifting $x \equiv 4 \pmod{11}$. Putting $x = 4+11a$ we find $a \equiv 3 \pmod{11}$ and hence $x \equiv 37 \pmod{11^2}$. Then putting $x = 37 + 11^2 a$ we find $a \equiv -1 \pmod{11}$ so $x \equiv -84 \equiv 1247 \pmod{11^3}$.
Hence the only solution of $x^3 + x^2 + 8 \equiv 0 \pmod{11^3}$ is $x \equiv -84 \pmod{11^3}$.

Total for question: [15]

2. In the lectures we showed that 3 is a primitive root of 19.
(i) We find that $7 \equiv 3^6 \bmod 19$. Set $x \equiv 3^t \pmod{19}$. Then $3^{5t} \equiv 3^6 \pmod{19}$ so that $5t \equiv 6 \pmod{18}$. Solving this gives $t \equiv 12 \bmod 18$. Thus $x \equiv 3^{12} \equiv 11 \bmod 19$.

(ii) We find that $4 \equiv 3^{14} \pmod{19}$. Set $x \equiv 3^t \pmod{19}$. Then $3^{4t} \equiv 3^{14} \pmod{19}$ so that $4t \equiv 14 \pmod{18}$. Solving this gives $t \equiv 8 \pmod 9$ or equivalently $t \equiv 8$ or $17 \pmod{18}$. Therefore $x \equiv 3^8$ or $3^{17} \pmod{19}$, that is $x \equiv \pm 6 \pmod{19}$.

(iii)* We find that $9 \equiv 3^2 \pmod{19}$. Set $x \equiv 3^t \pmod{19}$. Then $3^{10t} \equiv 3^2 \pmod{19}$ so that $10t \equiv 2 \pmod{18}$. This is equivalent to $5t \equiv 1 \pmod{9}$, and solving this gives $t \equiv 2 \bmod 9$ or equivalently $t \equiv 2$ or $11 \pmod{18}$. Therefore $x \equiv 3^2$ or $3^{11} \pmod{19}$, that is $x \equiv \pm 9 \pmod{19}$. **[5]**

Total for question: [5]

3. Let $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. We showed in lectures that for any $k \in \mathbb{Z}$, $\mathrm{ord}_n(a^k) = \mathrm{ord}_n(a)$ if and only if $\gcd(\mathrm{ord}_n(a), k) = 1$. In particular, if a is a primitive root mod n then $\mathrm{ord}_n(a) = \varphi(n)$ and so a^k is a primitive root if and only if $\gcd(\varphi(n), k) = 1$. But any $b \in \mathbb{Z}$ with $\gcd(b, n) = 1$ is congruent to a^k mod n for some $k \in \mathbb{Z}$ with $1 \leq k < \varphi(n)$. In particular, this is the case if we take b to be any primitive root. But the number of $k \in \mathbb{Z}$ with both $1 \leq k < \varphi(n)$ and $\gcd(\varphi(n), k) = 1$ is $\varphi(\varphi(n))$.

4*. We show that if g is a primitive root $\pmod p$ then $g + tp$ is a primitive root $\pmod{p^2}$ for exactly $p-1$ values of $t \pmod p$. Let h denote the order of $g + tp \pmod{p^2}$. (Thus h may depend on t). Since $(g+tp)^h \equiv 1 \pmod{p^2}$, it follows that $(g + tp)^h \equiv 1 \pmod p$, which in turn implies that $g^h \equiv 1 \pmod p$, and hence that $(p-1) \mid h$. On the other hand, by Corollary 2.60 (lecture notes) we know that $h \mid \varphi(p^2) = p(p-1)$. Thus $h = p - 1$ or $h = p(p-1)$. In the latter case $g + tp$ is a primitve root $\pmod{p^2}$, and in the former case it is not. We prove that the former case arises for only one of the p possible values of t. Let $f(x) = x^{p-1} - 1$. In the former case, $g + tp$ is a solution of the congruence $f(x) \equiv 0 \pmod{p^2}$ lying above $g \pmod p$. Since $f'(g) = (p-1)g^{p-2} \not\equiv 0 \pmod p$, we know from Hensel's lemma that $g \pmod p$ lifts to a unique solution $g + tp \pmod{p^2}$. For all other values of $t \pmod p$, the number $g + tp$ is a primitive root $\pmod{p^2}$.
Since each of the $\varphi(p-1)$ primitive roots $\pmod p$ give rise to exactly $p-1$ primitive roots $\pmod{p^2}$, we have now shown that there exist at least $(p-1)\varphi(p-1)$ primitive roots $\pmod{p^2}$. To show that there are no other primitive roots $\pmod{p^2}$, it suffices to argue as follows. Let g denote a primitive root $\pmod{p^2}$, so that the numbers $g, g^2, \cdots, g^{p(p-1)}$ form a system of reduced residues $\pmod{p^2}$. By Lemma 2.83 (lecture notes), we know that g^k is a primitive root if and only if $(k, p(p-1)) = 1$. By the definition of Euler's phi function, there are precisely $\varphi(p(p-1))$ such values of k among the numbers $1, 2, \cdots, p(p-1)$. Since $(p, p-1) = 1$, we deduce from Theorem 2.43 (lecture notes) that $\varphi(p(p-1)) = \varphi(p)\varphi(p-1) = (p-1)\varphi(p-1)$. **[15]**

Total for question: [15]

5. First, we can make an observation. Let a be any positive integer congruent to 1 modulo p. Then, by Wilson's theorem,

$$a(a+1)\cdots[a+(p-2)] \equiv (p-1)! \equiv -1 \pmod p.$$

In other words, the product of the $p-1$ integers between any two consecutive multiples of p is congruent to -1 modulo p. Then

$$\begin{aligned}
\frac{(np)!}{n!p^n} &= \frac{(np)!}{p\dot{2}p\dot{3}p\cdots(np)} \\
&= \prod_{r=1}^{n}[(r-1)p+1]\cdots[(r-1)p+(p-1)] \\
&\equiv \prod_{r=1}^{n}(p-1)! \pmod{p} \\
&\equiv \prod_{r=1}^{n}(-1) \pmod{p} \\
&\equiv (-1)^n \pmod{p}.
\end{aligned}$$

[10]

Total for question: [10]

6. Note: in the following solutions, I have not used the Jacobi symbol. However, several of the solutions could be simplified by using the Jacobi symbol and the corresponding law of quadratic reciprocity.

(i)*

$$\begin{aligned}
\left(\frac{3}{53}\right) &= \left(\frac{53}{3}\right) && \text{as } 53 \equiv 1 \pmod{4} \\
&= \left(\frac{-1}{3}\right) && \text{as } 53 \equiv -1 \pmod{3} \\
&= -1.
\end{aligned}$$

(ii)

$$\begin{aligned}
\left(\frac{7}{79}\right) &= -\left(\frac{79}{7}\right) && \text{as } 7 \equiv 79 \equiv 3 \pmod{4} \\
&= -\left(\frac{2}{7}\right) && \text{as } 79 \equiv 2 \pmod{7} \\
&= -(+1) && \text{as } 7 \equiv \pm 1 \pmod{8} \\
&= -1.
\end{aligned}$$

(iii)*

$$\begin{aligned}
\left(\frac{15}{101}\right) &= \left(\frac{3}{101}\right)\left(\frac{5}{101}\right) \\
&= \left(\frac{101}{3}\right)\left(\frac{101}{5}\right) && \text{as } 101 \equiv 1 \pmod{4} \\
&= \left(\frac{2}{3}\right)\left(\frac{1}{5}\right) \\
&= (-1)(+1) \\
&= -1.
\end{aligned}$$

(iv)

$$\begin{aligned}
\left(\frac{31}{641}\right) &= \left(\frac{641}{31}\right) \qquad \text{as } 641 \equiv 1 \pmod 4 \\
&= \left(\frac{21}{31}\right) \\
&= \left(\frac{3}{31}\right)\left(\frac{7}{31}\right) \\
&= \left[-\left(\frac{31}{3}\right)\right]\left[-\left(\frac{31}{7}\right)\right] \qquad \text{as } 3,\ 7,\ 31 \text{ are all} \equiv 3 \pmod 4 \\
&= \left[-\left(\frac{1}{3}\right)\right]\left[-\left(\frac{3}{7}\right)\right] \\
&= [-1]\left[+\left(\frac{7}{3}\right)\right] \qquad \text{as } 3,\ 7, \text{ are both} \equiv 3 \pmod 4 \\
&= -\left(\frac{1}{3}\right) \\
&= -1.
\end{aligned}$$

(v)

$$\begin{aligned}
\left(\frac{111}{991}\right) &= \left(\frac{3}{991}\right)\left(\frac{37}{991}\right) \\
&= -\left(\frac{991}{3}\right)\left(\frac{991}{37}\right) \qquad \text{as } 3 \equiv 991 \equiv 3 \pmod 4;\ 37 \equiv 1 \pmod 4 \\
&= -\left(\frac{1}{3}\right)\left(\frac{-8}{37}\right) \\
&= -(+1)\left(\frac{-1}{37}\right)\left(\frac{2}{37}\right)^3 \\
&= -(+1)(+1)(-1)^3 \qquad \text{as } 37 \equiv 1 \pmod 4 \text{ and } 37 \equiv -3 \pmod 8 \\
&= +1.
\end{aligned}$$

(vi)

$$\begin{aligned}
\left(\frac{105}{1009}\right) &= \left(\frac{3}{1009}\right)\left(\frac{5}{1009}\right)\left(\frac{7}{1009}\right) \\
&= \left(\frac{1009}{3}\right)\left(\frac{1009}{5}\right)\left(\frac{1009}{7}\right) \qquad \text{as } 1009 \equiv 1 \pmod 4 \\
&= \left(\frac{1}{3}\right)\left(\frac{4}{5}\right)\left(\frac{1}{7}\right) \\
&= (+1)(+1)(+1) \\
&= +1.
\end{aligned}$$

(vii)

$$\begin{aligned}
\left(\frac{77}{107}\right) &= \left(\frac{7}{107}\right)\left(\frac{11}{107}\right) \\
&= \left[-\left(\frac{107}{7}\right)\right]\left[-\left(\frac{107}{11}\right)\right] \qquad \text{as } 7,\ 11 \text{ and } 107 \text{ are all} \equiv 3 \pmod 4 \\
&= \left(\frac{2}{7}\right)\left(\frac{8}{11}\right) \\
&= (+1)\left(\frac{2}{11}\right)^3 \qquad \text{as } 7 \equiv -1 \pmod 8 \\
&= (-1)^3 \qquad \text{as } 11 \equiv 3 \pmod 8 \\
&= -1.
\end{aligned}$$

(viii)*

$$\begin{aligned}
\left(\frac{133}{191}\right) &= \left(\frac{7}{191}\right)\left(\frac{19}{191}\right) \\
&= \left[-\left(\frac{191}{7}\right)\right]\left[-\left(\frac{191}{19}\right)\right] \qquad \text{as } 7,\ 19 \text{ and } 191 \text{ are all} \equiv 3 \pmod 4 \\
&= \left(\frac{2}{7}\right)\left(\frac{1}{19}\right) \\
&= (+1)(+1) \qquad \text{as } 7 \equiv -1 \pmod 8 \\
&= +1.
\end{aligned}$$

(ix)*

$$\begin{aligned}
\left(\frac{-111}{257}\right) &= \left(\frac{-1}{257}\right)\left(\frac{3}{257}\right)\left(\frac{37}{257}\right) \\
&= (+1)\left(\frac{257}{3}\right)\left(\frac{257}{37}\right) \qquad \text{as } 257 \equiv 1 \pmod 4 \\
&= \left(\frac{2}{3}\right)\left(\frac{-2}{37}\right) \\
&= (-1)\left(\frac{-1}{37}\right)\left(\frac{2}{37}\right) \\
&= (-1)(+1)(-1) \qquad \text{as } 37 \equiv 1 \pmod 4 \text{ but } 37 \equiv -3 \pmod 8 \\
&= +1.
\end{aligned}$$

(x)

$$\begin{aligned}
\left(\frac{221}{347}\right) &= \left(\frac{13}{347}\right)\left(\frac{17}{347}\right) \\
&= \left(\frac{347}{13}\right)\left(\frac{347}{17}\right) \qquad \text{as } 13 \equiv 17 \equiv 1 \pmod 4 \\
&= \left(\frac{9}{13}\right)\left(\frac{7}{17}\right) \\
&= (+1)\left(\frac{17}{7}\right) \qquad \text{as } 17 \equiv 1 \pmod 4 \\
&= \left(\frac{3}{7}\right) \\
&= -\left(\frac{7}{3}\right) \qquad \text{as } 3,\ 7 \text{ are both} \equiv 1 \pmod 4 \\
&= -\left(\frac{1}{3}\right) \\
&= -1.
\end{aligned}$$

(xi)*

$$\begin{aligned}
\left(\frac{-257}{541}\right) &= \left(\frac{-1}{541}\right)\left(\frac{257}{541}\right) \\
&= (+1)\left(\frac{541}{257}\right) \qquad \text{as } 541 \equiv 1 \pmod 4 \\
&= \left(\frac{27}{257}\right) \\
&= \left(\frac{3}{257}\right)^3 \\
&= \left(\frac{257}{3}\right) \qquad \text{as } 257 \equiv 1 \pmod 4 \\
&= \left(\frac{2}{3}\right) \\
&= -1.
\end{aligned}$$

(xii)

$$\begin{aligned}
\left(\frac{511}{881}\right) &= \left(\frac{7}{881}\right)\left(\frac{73}{881}\right)\\
&= \left(\frac{881}{7}\right)\left(\frac{881}{73}\right) \qquad \text{as } 881 \equiv 1 \pmod 4\\
&= \left(\frac{-1}{7}\right)\left(\frac{5}{73}\right)\\
&= (-1)\left(\frac{73}{5}\right) \qquad \text{as } 7 \equiv 3 \pmod 4 \text{ and } 73 \equiv 1 \pmod 4\\
&= -\left(\frac{3}{5}\right)\\
&= -(-1)\\
&= +1.
\end{aligned}$$

3 marks per assessed part. Total for question: [15]

7. (i) To find $\left(\frac{7}{11}\right)$ by Gauss' Lemma, we need the least residues mod 11 of the first 5 multiples of 7, viz. 7, 14, 21, 28, 35. These least residues are 7, 3, 10, 6, 2. The number Λ with residues $> 11/2$ is 3, so

$$\left(\frac{7}{11}\right) = (-1)^3 = -1.$$

(ii) The least residues mod 13 of 5, 10, 15, 20, 25, 30 are 5, 10, 2, 7, 12, 4 respectively, so again $\Lambda = 3$ and

$$\left(\frac{5}{13}\right) = (-1)^3 = -1.$$

(iii) The least residues mod 17 of -3, -6, -9, -12, -15, -18, -21, -24 are 14, 11, 8, 5, 2, 16, 13, 10 respectively, so $\Lambda = 5$ and

$$\left(\frac{-3}{17}\right) = (-1)^5 = -1.$$

(iv) The least residues mod 19 of 5, 10, 15, 20, 25, 30, 35, 40, 45 are 5, 10, 15, 1, 6, 11, 16, 2, 7 respectively, so $\Lambda = 4$ and

$$\left(\frac{5}{19}\right) = (-1)^4 = +1.$$

8*. If $p = 2$, we have the solution $x = 1$. For any odd p, let p' denote its least positive residue modulo 13. Then

$$\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right) = \left(\frac{p^{'}}{13}\right),$$

so $p^{'}$ must be a quadratic residue modulo 13. A quick check shows that $p^{'} \equiv \pm 1, \pm 3, \pm 4 \bmod 13$.
Note also that $p = 13$ is a solution. **[10]**

Total for question: [10]

9. If $x^2 \equiv a \pmod p$ is soluble with $p \nmid a$, we have $\left(\frac{a}{p}\right) = +1$ by definition of the Legendre symbol, so $a^{(p-1)/2} \equiv +1 \pmod p$ by Euler's criterion. Now $(p+1)/4$ is an integer since $p \equiv 3 \pmod 4$, and for $x = \pm a^{(p+1)/4}$ we have

$$x^2 \equiv a^{(p+1)/2} \equiv aa^{(p-1)/2} \equiv a \pmod p.$$

Thus the solutions of $x^2 \equiv a \pmod p$ are $x \equiv \pm a^{(p+1)/4} \pmod p$. (We know that there are exactly two solutions mod p.)
Applying this to $x^2 \equiv 5 \pmod{79}$: we have $p = 79$ and $(p+1)/4 = 20$, so the solutions (if there are any) are $\pm 5^{20}$ mod 79. Now $5^{20} \equiv 20 \pmod{79}$, and we easily verify that $20^2 \equiv 5 \pmod{79}$. Hence the solutions are $x \equiv \pm 20 \pmod{79}$.

10*.
(i) We have $s(0,p) = \sum_{n=1}^{p} \left(\frac{n^2}{p}\right)$. By definition of the Legendre Symbol, $\left(\frac{n^2}{p}\right) = 1$ for all values of n for $1 \le n \le p-1$. For $n = p$, the Legendre symbol is zero thus $s(0,p) = \sum_{n=1}^{p} \left(\frac{n^2}{p}\right) = p - 1$. **[5]**

(ii) We have

$$\begin{aligned}
\sum_{a=1}^{p} s(a,p) &= \sum_{a=1}^{p}\sum_{n=1}^{p} \left(\frac{n(n+a)}{p}\right) \\
&= \sum_{n=1}^{p}\sum_{a=1}^{p} \left(\frac{n(n+a)}{p}\right) \\
&= \sum_{n=1}^{p}\sum_{b=1}^{p} \left(\frac{nb}{p}\right) \qquad \text{by the change of variable } b \equiv n + a \pmod p \\
&= \sum_{n=1}^{p}\sum_{b=1}^{p} \left(\frac{n}{p}\right)\left(\frac{b}{p}\right) \\
&= \sum_{n=1}^{p} \left(\frac{n}{p}\right) \sum_{b=1}^{p} \left(\frac{b}{p}\right) \\
&= \left(\sum_{n=1}^{p} \left(\frac{n}{p}\right)\right)^2.
\end{aligned}$$

Now $\sum_{n=1}^{p} \left(\frac{n}{p}\right) = 0$ since there are $(p-1)/2$ quadratic residues giving the value $(\frac{n}{p}) = 1$, plus $(p-1)/2$ quadratic non-residue giving the value $(\frac{n}{p}) = -1$, plus $(\frac{0}{p}) = 0$. **[5]**

(iii) In the sum $s(a,p) = \sum_{n=1}^{p} \left(\frac{n(n+a)}{p}\right)$, use the change of variables $b \equiv na^{-1} \pmod{p}$, so that $n \equiv ab \pmod{p}$, to rewrite

$$\begin{aligned}
s(a,p) &= \sum_{b=1}^{p} \left(\frac{ab(ab+a)}{p}\right) \\
&= \sum_{b=1}^{p} \left(\frac{a^2 b(b+1)}{p}\right) \\
&= \sum_{b=1}^{p} \left(\frac{a^2}{p}\right)\left(\frac{b(b+1)}{p}\right) \\
&= \sum_{b=1}^{p} \left(\frac{b(b+1)}{p}\right) \qquad \text{since } \left(\frac{a^2}{p}\right) = 1 \\
&= s(1,p).
\end{aligned}$$

[5]

(iv)Combining the previous parts, we find

$$\begin{aligned}
0 &= \sum_{a=1}^{p} s(a,p) \qquad \text{by part (ii)} \\
&= (p-1)s(1,p) + s(0,p) \qquad \text{by part (iii)} \\
&= (p-1)s(1,p) + (p-1) \qquad \text{by part(i)}.
\end{aligned}$$

Therefore $s(1,p) = -1$ and hence by part (iii), $s(a,p) = -1$ for all a such that $(a,p) = 1$. **[5]**

Total for question: [20]