ELEMENTARY NUMBER THEORY AND CRYPTOGRAPHY II
SOLUTIONS FOR PROBLEM SHEET 1
EPIPHANY TERM 2015

(1) (a) Since $5987 \equiv 3 \pmod 4$, we know that $\left(\frac{-1}{5987}\right) = -1$, and hence the congruence has no solution. (Note that 5987 is a prime.)

(b) Since $6780 \equiv -1 \pmod{6781}$ and the latter is $\equiv 1 \pmod 4$, we find $\left(\frac{-1}{6781}\right) = 1$, and so this congruence does have a solution. (Note that 6781 is a prime.)

(c) $x^2 + 14x - 35 \equiv 0$ can be rewritten as $(x+7)^2 \equiv 84$, so we need to figure out whether 84 is a QR modulo 337. We get

$$\left(\frac{84}{337}\right) = \left(\frac{2^2}{337}\right)\left(\frac{3}{337}\right)\left(\frac{7}{337}\right),$$

and invoking the quadratic reciprocity law, we find that

$$\left(\frac{3}{337}\right) = +\left(\frac{337}{3}\right) = +\left(\frac{1}{3}\right) = +1$$

as well as

$$\left(\frac{7}{337}\right) = +\left(\frac{337}{7}\right) = +1$$

and so the answer is yes, as

$$\left(\frac{84}{337}\right) = 1 \cdot 1 \cdot 1 = 1\,.$$

[In fact, since $74^2 \equiv 84 \pmod{337}$, the natural answer is $x = 74 - 7 = 67$.]

(d) We rewrite it as $(x-32)^2 - 32^2 + 943 = (x-32)^2 - 81 \equiv 0$ which obviously has solutions $x - 32 \equiv \pm 9 \pmod{3011}$ so one possibility is $x = 41$, and another one is $x = 23$.

(2) (a) The quadratic residues are (the classes of) 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18, while the non-residues are given by their negatives modulo 23 (as -1 is not a square mod 23).

(b) Since 7 is a NR and $7^{10} = (7^5)^2$ is a QR modulo 23, we know that $7^{11} = \mathrm{NR} \times \mathrm{QR} = \mathrm{NR}$.

(c) Since 2 is a QR and 5 is a NR modulo 23, we get $\left(\frac{2}{23}\right) = 1$ and $\left(\frac{5}{23}\right) = -1$, so using the multiplicativity of the Legendre symbol we find, for any $k, \ell \in \mathbb{Z}$

$$\left(\frac{2^k \cdot 5^\ell}{23}\right) = \left(\frac{2}{23}\right)^k \left(\frac{5}{23}\right)^\ell = (-1)^\ell\,.$$

(Note that $(-1)^a = (-1)^{-a}$.)

(3) (a) We count the number of integers with residue larger 11/2 in $\{8 \equiv 8, 16 \equiv 5, 24 \equiv 2, 32 \equiv 10, 40 \equiv 7\}$ which turns out to be 3, hence $\left(\frac{8}{11}\right) = -1$.

(b) Similarly, we find $\{7, 1, 8, 2, 9, 3\}$, and again $\left(\frac{7}{13}\right) = -1$.

(c) Here we get $\{5, 10, 15, 1, 6, 11, 16, 2, 7\}$, and so $\left(\frac{5}{19}\right) = 1$ (indeed, e.g. $81 \equiv 5 \pmod{19}$).

(d) Finally, we find $\{6, 12, 18, 24, 30, 5, 11, 17, 23, 29, 4, 10, 16, 22, 28\}$, and hence $\left(\frac{6}{31}\right) = -1$.

(4) Note that for an odd prime p, $\frac{p-1}{2}$ is even if and only if $p \equiv 1 \pmod 4$.

(a) Using that $101 \equiv 1 \pmod 4$, we get

$$\left(\frac{65}{101}\right) = \left(\frac{5}{101}\right)\left(\frac{13}{101}\right) = \left(\frac{101}{5}\right)\left(\frac{101}{13}\right) = \left(\frac{1}{5}\right)\left(\frac{2}{13}\right)\left(\frac{5}{13}\right) =$$

$$= (-1)^{\frac{13^2-1}{8}}\left(\frac{13}{5}\right) = -\left(\frac{3}{5}\right) = 1\,.$$

Here we have used $\left(\frac{2}{p}\right)(-1)^{\frac{p^2-1}{8}}$ for an odd prime p, which we have seen is equivalent to

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & if\ p \equiv \pm 1 \pmod 8 \\ -1 & if\ p \equiv \pm 3 \pmod 8 \end{cases}$$

(b) Using again that $101 \equiv 1 \pmod 4$, we get

$$\left(\frac{101}{2011}\right) = \left(\frac{2011}{101}\right) = \left(\frac{-9}{101}\right) = \left(\frac{-1}{101}\right) = 1\,.$$

(c) In a similar way, we consider

$$\left(\frac{111}{641}\right) = \left(\frac{3}{641}\right)\left(\frac{37}{641}\right) = \left(\frac{641}{3}\right)\left(\frac{641}{37}\right) = \left(\frac{2}{3}\right)\left(\frac{3}{37}\right)\left(\frac{2^2}{37}\right) = -1\,,$$

since 2 is quadratic non-residue modulo 3, and $\left(\frac{3}{37}\right) = \left(\frac{37}{3}\right)$ ⟦as $37 \equiv 1 \pmod 4$⟧ which is obviously a quadratic residue modulo 3 ⟦as 37 is also congruent to 1 modulo 3⟧.

(d) Finally, $\left(\frac{31706}{43789}\right) = -1$ (note $31706 = 2 \cdot 83 \cdot 191$ and check that $\left(\frac{2}{43789}\right) = -1$, $\left(\frac{83}{43789}\right) = \left(\frac{191}{43789}\right) = 1$).

(5) Since $3 \equiv 3 \pmod 4$ the Quadratic Reciprocity Law implies that

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & if\ p \equiv 1 \pmod 4 \\ -\left(\frac{p}{3}\right) & if\ p \equiv 3 \pmod 4 \end{cases}$$

But $p \equiv 1 \pmod 3$ or $p \equiv 2 \pmod 3$. Hence in the first case we have $\left(\frac{p}{3}\right) = 1$ and in the second case we have $\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$. Hence we have that $\left(\frac{3}{p}\right) = 1$ if and only if ($p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 3$) or ($p \equiv 3 \pmod 4$ and $p \equiv 2 \pmod 3$). The first condition is equivalent to $p \equiv 1 \pmod{12}$ and the second to $p \equiv -1 \pmod{12}$ (why?). Hence $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{12}$. for the rest, namely $p \equiv \pm 5 \pmod{12}$ we have that it is -1.

(6) (a) We first note that $4^m \equiv 4 \pmod{12}$ for any m. Indeed this is clear for $m = 1$, and for $m \geq 2$ we have $4^m - 4 == 4(4^{m-1} - 1) = 4(4 - 1)(4^{m-2} + \cdots + 1)$, and hence it is divisible by 12. Then we have

$$F_n \equiv 2^{2^n} + 1 \equiv 2^{2m} + 1 \equiv 4^m + 1 \equiv 4 + 1 \equiv 5 \pmod{12}$$

(b) This follows by the previous question immediately.

(c) By the Eule's Criterion we have that $3^{\frac{F_n-1}{2}} \equiv \left(\frac{3}{F_n}\right) \equiv -1 \pmod{F_n}$. But since we are taking F_n prime we have that $\phi(F_n) = F_n - 1$, and hence we obtain $3^{\frac{\phi(F_n)}{2}} \equiv -1 \pmod{F_n}$. From this we conclude that 3 has order $\phi(F_n)$ and hence is a primitive root modulo F_n. Indeed for this it is enough to observe that $\phi(F_n) - 1 = 2^{2^n}$ has only 2 as a prime in its prime factorization, hence we need to check only whether $3^{\frac{F_n-1}{2}} \not\equiv 1 \pmod{F_n}$.

(7) (a) Consider a prime divisor p of $n^2 + 1$. Then we have

$$n^2 \equiv -1 \pmod{p}$$

or in other words -1 is QR modulo p. If $p = 2$ there is nothing to show. If p is odd then p has to be congruent to 1 modulo 4.

(b) Suppose that there are only finitely many primes of the form $4k + 1$. Let these be $p_1, p_2, \ldots, p_n$. Consider the number

$$N = (2 \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_n)^2 + 1.$$

By part (a) every prime divisor q of N must be of the form $4k + 1$ (cannot be two since N is odd). However q is coprime to all numbers $p_1, p_2, \ldots, p_n$. Therefore q is not in the list, and so we derive a contradiction.

(8) This is similar as the last one. Assume there is a finite number of such primes, say $p_1, \ldots, p_n$, and consider the $N := (4p_1p_2 \cdots p_n)^2 - 2$. There exists at least one odd prime divisor of (since N cannot be a power of 2), which implies that $(4p_1p_2 \cdots p_n)^2 \equiv 2 \pmod{p}$ or equivalently that $\left(\frac{2}{p}\right) = 1$, and hence $p \equiv \pm 1 \pmod{8}$. If all prime divisors of N were of the form $8k + 1$, then N would have been of the form $16m + 2$, which is not possible since N is of the form $16m - 2$. Hence there is at least one prime divisor of the form $8k - 1$, and this cannot be any of the ones in teh list. Contradiction.

(9) (a) This is clear since if $x^2 \equiv a \pmod{p^k}$ has a solution, then so has also $x^2 \equiv a \pmod{p}$.

(b) We compute

$$(x_k + y_p^k)^2 = x_k^2 + 2x_k y p^k + y^2 p^{2k} = a + (b + 2x_k y)p^k + y^2 p^{2k}$$

Taking now modulo p^{k+1}, and using the fact that $b + 2x_k y \equiv 0 \pmod{p}$ we conclude that $x_{k+1}^2 \equiv a \pmod{p^{k+1}}$.

(c) The theorem follows now by induction, where the inductive step is as above.

(10) (a) It is enough to observe that the square of an odd integer is congruent to one modulo 4. And if we are given an a with $a \equiv 1 \pmod{4}$, then we can take as solution 1 or 3.

(b) We first observe that the square of an odd integer is always congruent to 1 modulo 8 (Check). Hence if the equation $x^2 \equiv a \pmod{2^n}$ with $n \geq 3$ has a solution then $a \equiv 1 \pmod 8$. For the other direction we argue as in the previous exercise (9), and use induction. When $n = 3$ we can always find a solution to the equation $x^2 \equiv 1 \pmod 8$, actually all $1, 3, 5, 7$ are solutions. Now we take an $n > 3$ and assume for the induction hypothesis that the congruence $x^2 \equiv a \pmod{2^n}$ has a solution x_n. We write $x_n^2 = a + b2^n$, and since a is odd, we have that so is x_n. Hence we can solve $x_n y \equiv -b \pmod 2$ to find a y, and then set $x_{n+1} = x_n + y2^{n-1}$. Then one can check, exactly as in (9) that $x_{n+1}^2 \equiv a \pmod{2^{n+1}}$, and hence finishing the induction.

(11) This follows by combining the exercises (9) and (10) above. Indeed we notice that the equation $x^2 \equiv a \pmod n$ has a solution if and only if the equations $x^2 \equiv a \pmod{2^{k_0}}$, $x^2 \equiv a \pmod{p_1^{k_1}}, \ldots, x^2 \equiv a \pmod{p_r^{k_r}}$ all have a solution. If $k_0 = 1$ there is no condition on the first congruence in order to have a solution. The other cases follow from (9) and (10) above.