Elementary Number Theory and Cryptography, Epiphany 2015

Problem Sheet 1, (Due: Monday Jan 26, at 12:00 in CM116)

Please hand in Problems 1(b), 2(a,b), 3(a), 4(a), 5.
The Problems 1(a), 4(b), 6, 7, 9 will be discussed in the tutorials, (depending on time).

1. Determine whether each of the following congruences has a solution in integers.
   (a) $x^2 \equiv -1 \pmod{5987}$,
   (b) $x^2 \equiv 6780 \pmod{6781}$,
   (c) $x^2 + 14x - 35 \equiv 0 \pmod{337}$,
   (d) $x^2 - 64x + 943 \equiv 0 \pmod{3011}$.

2. (a) Produce a list of all the QRs and NRs modulo the prime 23.
   (b) Is 7^{11} a QR modulo 23? Justify your answer.
   (c) Determine
   $$\left(\frac{2^k \cdot 5^\ell}{23}\right)$$
   for arbitrary k, $\ell \in \mathbb{N}$. [Your answer will depend on ℓ and k].

3. Use Gauss lemma to evaluate each of the following Legendre symbols
   $$(a)\ \left(\frac{8}{11}\right) \qquad (b)\ \left(\frac{7}{13}\right) \qquad (c)\ \left(\frac{5}{19}\right) \qquad (d)\ \left(\frac{6}{31}\right).$$

4. Compute the following Legendre symbols:
   $$(a)\ \left(\frac{65}{101}\right) \qquad (b)\ \left(\frac{101}{2011}\right) \qquad (c)\ \left(\frac{111}{641}\right) \qquad (d)\ \left(\frac{31706}{43789}\right).$$

5. Let $p \neq 3$ be an odd prime. Show that
   $$\left(\frac{3}{p}\right) = \begin{cases} 1 & : p \equiv \pm 1 \pmod{12} \\ -1 & : p \equiv \pm 5 \pmod{12} \end{cases}$$

6. Write $F_n = 2^{2^n} + 1$ for $n > 1$. Show that
   (a) $F_n \equiv 5 \pmod{12}$,
   (b) Assume that F_n is a prime. By using question 5 above conclude that $\left(\frac{3}{F_n}\right) = -1$.
   (c) Show that 3 is a primitive root modulo F_n when F_n is a prime number.

7. (a) Let $n \in \mathbb{N}$. Show that for each prime divisor p of the number n^2+1 we have either $p = 2$ or $p \equiv 1 \pmod 4$. [Hint: show that -1 is a QR modulo p].

   (b) By using (a) or otherwise show that there are infinitely many primes of the form $4k+1$, $k \in \mathbb{N}$.

8. Show that there are infinitely many primes of the form $8n-1$ for $n \in \mathbb{N}$. [Hint: Assume there exist finitely many, say $p_1, p_2, \cdots, p_k$, and consider the integer $N = (4p_1p_2 \dots p_k)^2 - 2$].

9. The aim of the following exercise is to prove the following theorem

   Theorem: If p is an odd prime and $gcd(a,p) = 1$, then the congruence

   $$x^2 \equiv a \pmod{p^n}$$

   for $n \geq 1$ has a solution if and only if $\left(\frac{a}{p}\right) = 1$. Show the following

   (a) Show that if $x^2 \equiv a \pmod{p^n}$ has a solution then $\left(\frac{a}{p}\right) = 1$.

   (b) Assume that $x_k \in \mathbb{Z}$ is a solution of $x^2 \equiv a \pmod{p^k}$ for some $k \in \mathbb{N}$. Show that $x_{k+1} := x_k + yp^k$ is a solution of the congruence $x^2 = a \pmod{p^{k+1}}$. Here y is defined as follows: Write $x_k^2 = a + bp^k$, and let y be defined by the equation $2x_k y \equiv -b \pmod p$ (Why is this well-defined?).

   (c) Conclude the theorem.

10. (a) Let a be an odd integer. Show that $x^2 \equiv a \pmod 4$ has a solution if and only if $a \equiv 1 \pmod 4$.

    (b) Show that $x^2 \equiv a \pmod{2^n}$ for $n \geq 3$ has a solution if and only if $a \equiv 1 \pmod 8$.

11. Let $n \in \mathbb{N}$ and assume $n = 2^{k_0}p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$, with $p_i \neq p_j$ for $i \neq j$. For an $a \in \mathbb{Z}$ with $gcd(a,n) = 1$ show that the equation

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

    is solvable if and only if $\left(\frac{a}{p}\right) = 1$ for $i = 1, 2, \dots r$ and

    $$a \equiv \begin{cases} 1 \pmod 4 & : k_0 = 2 \\ 1 \pmod 8 & : k_0 \geq 3 \end{cases}$$