Number Theory, Spring 2014.
Solutions to the second midterm

1. Let p be an odd prime, and let $x \in \mathbb{Z}$ be a primitive root mod p.

(a) (2 pts) Prove that x is a primitive root mod $p^2 \iff x^{p-1} \not\equiv 1 \mod p^2$.

(b) (4 pts) Let $i \in [1, p-1]$. Use (a) and the lifting theorem to prove that x or $x + ip$ is a primitive root mod p^2.

(c) (4 pts) Assume that $p \equiv 1 \mod 4$. Prove that $-x$ is also a primitive root mod p.

(d) (2 pts) Use (a), (b) and (c) to prove that if $p \equiv 1 \mod 4$, then there exists $y \in [1, p-1]$ which is a primitive root mod p^2.

Solution: (a) "$\Rightarrow$" Suppose that x is a primitive root mod p^2, so $[x]_{p^2}$ has order $|U_{p^2}| = p(p-1)$. Hence for any $0 < m < p(p-1)$ we have $([x]_{p^2})^m \neq [1]_{p^2}$, so $x^m \not\equiv 1 \mod p^2$. In particular, $x^{p-1} \not\equiv 1 \mod p^2$.

"$\Leftarrow$" Conversely, suppose that $x^{p-1} \not\equiv 1 \mod p^2$. Since x is a primitive root mod p, we have $o([x]_p) = p-1$.

Let $a = o([x]_{p^2})$. Since $[x]_{p^2}^a = [1]_{p^2}$, we have $[x]_p^a = [1]_p$, so $p-1 = o([x]_p)$ divides a. On the other hand, by Lagrange theorem, a divides $|U|_{p^2} = p(p-1)$. The only positive integers which are divisible by $p-1$ and divide $p(p-1)$ are $p-1$ and $p(p-1)$.

Since $x^{p-1} \not\equiv 1 \mod p^2$, we know that $a \neq p-1$. Thus, we must have $a = p(p-1)$, whence $[x]_{p^2}$ is a generator of U_{p^2} and so x is a primitive root mod p^2.

(b) Let $f(t) = t^{p-1} - 1$. Since $f(x) \equiv 0 \mod p$ while $f'(x) = (p-1)x^{p-2}$ is not divisible by p, by the lifting theorem, there is unique $y \in [0, p^2)$ such that $y \equiv x \mod p$ and $f(y) \equiv 0 \mod p^2$.

If $y \neq x$, then $x^{p-1} \not\equiv 1 \mod p^2$, so by (a), x is a primitive root mod p^2. And if $y = x$, then $(x + ip)^{p-1} \not\equiv 1 \mod p^2$ for any $i \in [1, p-1]$, so $x + ip$ is a primitive root mod p^2.

(c) Let $k = o([-x]_p)$. We need to prove that $k = p-1$. Suppose, on the contrary, that $k < p-1$. By definition of the order we have $(-x)^k \equiv 1 \mod p$, so $x^k \equiv (-1)^k \mod p$. If k is even, this would imply that $o([x])_p \leq k < p-1$, contradicting the assumption that x is a primitive root mod p.

Thus, k is odd. Squaring both sides of $x^k \equiv (-1)^k \mod p$, we get $x^{2k} \equiv 1 \mod p$, so $[x]_p^{2k} = [1]_p$. Since $[x]_p$ is a generator of U_p and $|U_p| = p-1$, we deduce that $(p-1) \mid 2k$. This is impossible since $p \equiv 1 \mod 4$ while k is odd.

(d) We know that there exists $z \in [1, p-1]$ which is a primitive root mod p. If z is a primitive root mod p^2, we are done. Suppose now that z is not a primitive root mod p^2. Then $z^{p-1} \equiv 1 \mod p^2$ by (a). Since p is even, we have $(-z)^{p-1} \equiv 1 \mod p^2$, so again by (a), $-z$ is not a primitive root mod p^2; on the other hand, by (c), $-z$ is primitive root mod p. Thus, applying (b) to $x = -z$, we conclude that $-z + p$ is a primitive root mod p^2. Since $-z + p \in [1, p-1]$, the proof is complete.

2.

(a) (2 pts) Let n and d be positive integers. Let G be a finite cyclic group of order n. What is the number of solutions to the equation $g^d = e$ in G as a function of n and d? An answer is sufficient.

(b) (6 pts) Let $p_1, \ldots, p_k$ be distinct odd primes, let $n = p_1 \ldots p_k$ and define $m_i = \frac{p_i - 1}{2}$. Suppose that $m_1, \ldots, m_k$ are pairwise coprime. Prove that for every prime $p > 2$, the congruence $x^p \equiv 1 \mod n$ has at most p reduced solutions.

(c) (4 pts) Prove that for any $k \in \mathbb{N}$, there exist k primes satisfying the hypothesis of (b).

Solution: (a) $gcd(n, d)$.

(b) For a positive integer l denote by $f(l)$ the number of reduced solutions to $x^p \equiv 1 \mod l$. Since $p_1, \ldots, p_k$ are pairwise coprime, we have $f(n) = f(p_1) \ldots f(p_k)$.

If q is prime, the number of reduced solutions to $x^p \equiv 1 \mod q$ is equal to the number of solutions to $g^p = e$ in U_q, which is a cyclic group of order $q-1$. Hence by (a) for each i we have $f(p_i) = gcd(p, p_i - 1)$. Thus $f(p_i) = p$ if $p \mid (p_i - 1)$ and $f(p_i) = 1$ otherwise.

Since p is odd and the numbers $\frac{p_1-1}{2}, \ldots, \frac{p_k-1}{2}$ are pairwise coprime, there is at most one i for which $p \mid (p_i - 1)$. Therefore, $f(n) = f(p_1) \ldots f(p_k) = 1$ or p.

(c) We use induction on k. The statement trivially holds for $k = 1$. Now suppose that k is arbitrary and we have constructed primes $p_1, \ldots, p_k$ such that the integers $m_1 = \frac{p_1-1}{2}, \ldots, m_k = \frac{p_k-1}{2}$ are pairwise coprime. We shall prove that there is a prime p_{k+1} such that $m_{k+1} = \frac{p_{k+1}-1}{2}$ is coprime to $m_1, \ldots, m_k$.

Let $m = m_1 \ldots m_k$. Since $gcd(2m, -1) = 1$, by Dirichlet's theorem, there exists $l \in \mathbb{N}$ such that $p_{k+1} = 2ml - 1$ is prime. Then $m_{k+1} = (2ml - 2)/2 = ml - 1$ is coprime to m, so in particular coprime to each of the numbers $m_1, \ldots, m_k$.

3. (a) (3 pts) Let $n \in \mathbb{N}$ be odd, and suppose that the congruence $x^2 \equiv 2 \mod n$ has a solution. Prove that $n \equiv 1$ or $7 \mod 8$.

Now let q be an odd prime. As in HW#8.2, define $N = q$ if $q \equiv 1 \mod 4$ and $N = 4q$ if $q \equiv 3 \mod 4$. If $q \equiv 1 \mod 4$, define $A = Q_q$, the group of quadratic residues mod q (thought of as a subgroup of U_q) and $B = U_q \setminus A$. If $q \equiv 3 \mod 4$, define

$$A(1) = \{[x]_{4q} \in U_{4q} : x \equiv 1 \mod 4 \text{ and } [x]_q \in Q_q\},$$
$$A(2) = \{[x]_{4q} \in U_{4q} : x \equiv 3 \mod 4 \text{ and } [x]_q \notin Q_q\},$$

$A = A(1) \cup A(2)$ and $B = U_{4q} \setminus A$.

(b) (3 pts) Prove that if p is an odd prime distinct from q, then

$$\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } [p]_N \in A \\ -1 & \text{if } [p]_N \in B \end{cases}$$

(c) (3 pts) Prove that A is a subgroup of U_N.

(d) (3 pts) Use (b) and (c) to prove that there exists an integer r such that the congruence $x^2 \equiv q \mod n$ has no solutions for any **odd** integer n satisfying $n \equiv r \mod N$. **Hint:** your argument should be similar to the one in (a) except that things will be less explicit.

Solution: (a) Let p be a prime divisor of n. Since n is odd, p is also odd. Also, by assumption there exists $x \in \mathbb{Z}$ such that $x^2 \equiv 2 \mod n$, so $x^2 \equiv 2 \mod p$ as well and therefore by the formula for $(\frac{2}{p})$ proved in class, we conclude that $p \equiv 1$ or $7 \mod 8$.

Hence n is a product of primes congruent to 1 or 7 mod 8. Since the set $\{[1]_8, [7]_8\}$ is a subgroup of U_8, it follows that n itself is congruent to 1 or 7 mod 8.

(b) If $q \equiv 1 \mod 4$, then $(\frac{q}{p}) = (\frac{p}{q})$, which by definition equals 1 if $[p]_q \in A$ and -1 if $[p]_q \in B$.

Now suppose that $q \equiv 3 \mod 4$. Then $(\frac{q}{p}) = \begin{cases} (\frac{p}{q}) & \text{if } p \equiv 1 \mod 4 \\ -(\frac{p}{q}) & \text{if } p \equiv 3 \mod 4 \end{cases}$

Thus, $(\frac{q}{p}) = 1 \iff$ one of the following holds:

(i) $(\frac{p}{q}) = 1$ (that is, $[p]_q \in Q_q$) and $p \equiv 1 \mod 4$

(ii) $(\frac{p}{q}) = -1$ (that is, $[p]_q \notin Q_q$) and $p \equiv 3 \mod 4$.

By definition, (i) holds $\iff [p]_{4q} \in A(1)$ and (ii) holds $\iff [p]_{4q} \in A(2)$. Thus, $(\frac{q}{p}) = 1 \iff [p]_{4q} \in A$ (and therefore, $(\frac{q}{p}) = -1 \iff [p]_{4q} \notin A \iff [p]_{4q} \in B$).

(c) We already know that Q_q is a subgroup of U_q, so it suffices to consider the case $q \equiv 3 \mod 4$.

We shall use the following standard fact in group theory: if G is a finite group and H a non-empty subset of G which is closed under group operation, then H is necessarily a subgroup (that is, H is automatically closed under inversion).

Thus, it suffices to prove that if $[x]_N \in A$ and $[y]_N \in A$, then $[xy]_N \in A$. We consider four cases:

Case 1: $[x]_q, [y]_q \in Q_q$ and $x \equiv y \equiv 1 \mod 4$. Then $(\frac{x}{q}) = (\frac{y}{q}) = 1$, so $(\frac{xy}{q}) = (\frac{x}{q})(\frac{y}{q}) = 1$ (so $[xy]_q \in Q_q$) and $xy \equiv 1 \mod 4$, hence $[xy]_{4q} \in A(1)$.

Case 2: $[x]_q, [y]_q \notin Q_q$ and $x \equiv y \equiv 3 \mod 4$. Then $(\frac{x}{q}) = (\frac{y}{q}) = -1$, so $(\frac{xy}{q}) = (-1)^2 = 1$ (so $[xy]_q \in Q_q$) and $xy \equiv 3 \cdot 3 \equiv 1 \mod 4$, hence $[xy]_{4q} \in A(1)$.

Case 3: $[x]_q \in Q_q$, $x \equiv 1 \mod 4$, $[y]_q \notin Q_q$ and $y \equiv 3 \mod 4$. Then $(\frac{xy}{q}) = (\frac{x}{q})(\frac{y}{q}) = 1 \cdot (-1) = -1$ (so $[xy]_q \notin Q_q$) and $xy \equiv 3 \mod 4$, hence $[xy]_{4q} \in A(2)$.

Case 4: $[x]_q \notin Q_q$, $x \equiv 3 \mod 4$, $[y]_q \in Q_q$ and $y \equiv 1 \mod 4$. This case is analogous to Case 3.

(d) Fix any integer r coprime to N such that $[r]_N \notin A$. We claim that for any n such that $n \equiv r \mod N$ there congruence $x^2 \equiv q \mod n$ has no solution. Suppose, on the contrary, that there exists n such that $n \equiv r \mod N$ and $x^2 \equiv q \mod n$ for some x.

Let p be an arbitrary prime divisor of n. Then p is odd (since n is odd) and p is distinct from q (if $p = q$, then, since $q \mid (n-r)$, we also have $q \mid r$, so r is not coprime to N, which is a contradiction). Also, the congruence $x^2 \equiv q \mod p$ has a solution. Therefore, by definition $(\frac{q}{p}) = 1$, hence $[p]_N \in A$ by (b).

Let $p_1^{e_1} \dots p_s^{e_s}$ be the prime factorization of n. We just showed that $[p_i]_N \in A$ for each i, and since A is a subgroup, we conclude that $[n]_N = \prod [p_i]_N^{e_i} \in A$. On the other hand, since $n \equiv r \mod N$ and $[r]_N \notin A$, we must also have $[n]_N \notin A$, which is a contradiction.

4. (a) (4 pts) Let $p_1, \dots, p_k$ be distinct primes, and let $\varepsilon_1, \dots, \varepsilon_k$ be integers each of which is equal to ± 1. Prove that there exists a prime p such that $\left(\frac{p_i}{p}\right) = \varepsilon_i$ for each i. **Hint:** your computation will be easier if you impose an additional restriction on p right away. Problem 3 is relevant here.

Given an integer n and a prime $p > n$, define $f_p(n)$ to be the number of integers in the interval $[1, n]$ which are quadratic residues mod p. Define $f(n)$ to be the smallest possible value of $f_p(n)$ as p ranges over all possible primes $> n$.

We will say that n is *square-friendly* if $f(n) \geq n/2$, that is, for every prime $p > n$, at least half of integers in $[1, n]$ are quadratic residues mod p (note that different integers may serve as quadratic residues for different p). For instance, 4 is square-friendly since $\left(\frac{1}{p}\right) = \left(\frac{4}{p}\right) = 1$ for all p, so $f(4) \geq 2$. On the other hand, 3 is not square-friendly since $\left(\frac{2}{19}\right) = \left(\frac{3}{19}\right) = -1$, so $f(3) \leq f_{19}(3) \leq 1$.

(b) (4 pts) Prove that 10 is square-friendly, that is, $f(10) \geq 5$. **Hint:** This can be proved by case-by-case analysis. If you know the value $\left(\frac{q}{p}\right)$ for every prime $q < 10$, then you know $\left(\frac{n}{p}\right)$ for all $n \leq 10$.

(c) (4 pts) Prove that 100 is not square-friendly, that is, $f(100) < 50$. If you cannot prove this, try to prove as good an upper bound for $f(100)$ as you can. **Hint:** start by listing all primes between 1 and 100 (there are 25 of them).

Solution: (a) First, we observe that Dirichlet's theorem on primes in arithmetic progressions can be reformulated as follows. Suppose that integers b and r are coprime. Then there exists a prime p such that $p \equiv r \mod b$. We shall use Dirichlet's theorem in this form.

For simplicity, we first consider the case when none of p_i's is equal to 2. For each $1 \leq i \leq k$ choose $r_i \in \mathbb{Z}$ such that $(\frac{r_i}{p_i}) = \varepsilon_i$. By CRT there exists $r \in \mathbb{Z}$ such that $r \equiv r_i \mod p_i$ for each i and $r \equiv 1 \mod 4$.

Now let $b = 4p_1 \dots p_k$. Then by construction r is coprime to 4 and each p_i, so r is coprime to b. Hence, by Dirichlet's theorem there exists a prime p such that $p \equiv r \mod b$. We claim that p has required properties.

Indeed, by construction, $p \equiv 1 \mod 4$ and $p \equiv r_i \mod p_i$ for each i, whence

$$\left(\frac{p_i}{p}\right) = \left(\frac{p}{p_i}\right) = \left(\frac{r_i}{p_i}\right) = \varepsilon_i,$$

as desired.

In the case when one of the primes p_i is equal to 2 (WOLOG $p_1 = 2$) we use essentially the same argument except that we slightly modify the definition of r. First we choose $r_i \in \mathbb{Z}$ for $2 \le i \le k$ such that $(\frac{r_i}{p_i}) = \varepsilon_i$ and then define r to be any integer such that $r \equiv r_i \mod p_i$ for each $2 \le i \le k$ and $r \equiv \begin{cases} 1 \mod 8 & \text{if } \varepsilon_1 = 1 \\ 5 \mod 8 & \text{if } \varepsilon_1 = -1. \end{cases}$

(b) Let p be any prime > 10. Since $1, 4$ and 9 are perfect squares, we have $(\frac{1}{p}) = (\frac{4}{p}) = (\frac{9}{p}) = 1$, so all we need to show is among $2, 3, 5, 6, 7, 8, 10$ there are at least two quadratic residues mod p.

If $(\frac{2}{p}) = 1$, then $(\frac{8}{p}) = (\frac{2}{p})^3 = 1$, so 2 and 8 are quadratic residues mod p.

If $(\frac{2}{p}) = -1$, then $(\frac{6}{p}) = -(\frac{3}{p})$, so either $(\frac{3}{p}) = 1$ or $(\frac{6}{p}) = 1$ and similarly $(\frac{5}{p}) = 1$ or $(\frac{10}{p}) = 1$. Hence at least two of the integers $3, 5, 6, 10$ are quadratic residues mod p.

(c) We shall give several different solutions.

Let $p_1, \ldots, p_{25}$ be all the primes ≤ 100. By (a), for any sequence $\varepsilon_1, \ldots, \varepsilon_{25}$ of 1's and -1's, there exists a prime p such that $(\frac{p_i}{p}) = \varepsilon_i$ for each i. Note that if we know the values $(\frac{p_i}{p})$ for $1 \le i \le 25$, then (by multiplicativity of the Legendre symbol in the numerator), we know the values $(\frac{n}{p})$ for all $1 \le n \le 100$. Thus, we only need to find a sequence of ε_i's which forces more than 50 integers in $[1, 100]$ to be quadratic non-residues mod p.

One possibility is to take $\varepsilon_i = -1$ for each i. Then for $n \in [1, 100]$ we have $(\frac{n}{p}) = (-1)^{f(n)}$ where $f(n)$ is the number of distinct prime divisors of n (so $(\frac{n}{p}) = -1 \iff f(n)$ is odd). By direct computation there are 51 values of $n \in [1, 100]$ for which $f(n)$ is odd.

A slightly more elegant choice is to take $\varepsilon_1 = 1$ and $\varepsilon_i = -1$ for $2 \le i \le 25$ (that is, require that $(\frac{2}{p}) = 1$ and $(\frac{p_i}{p}) = -1$ for $2 \le i \le 25$). Then $(\frac{n}{p}) = -1$ whenever $n = 2^j p_i$ for some j and $2 \le i \le 25$.

Thus, to get a quadratic non-residue mod p, we can take n to be any of the p_i's (24 choices) or $n = 2p_i$ where p_i is a prime between 3 and 50 (14 choices) or $n = 4p_i$ where p_i is a prime between 3 and 25 (8 choices) or $n = 8p_i$ where p_i is a prime between 3 and 12 (4 choices) or $n = 16p_i$ where p_i is a prime between 3 and 6 (2 choices) or $n = 32 \cdot 3$ (1 choice). In total we have $24 + 14 + 8 + 4 + 2 + 1 = 53 > 50$ choices.

We finish with what is perhaps the most elegant solution, given in one of the exam papers. The idea is very simple. Let p be a prime which is larger than but close to 100. Then we know that among the integers $1, \ldots, p-1$ precisely half are quadratic residues mod p. Hence if we manage to prove that more than half of elements in $[101, p-1]$ are quadratic residues mod p (which can be checked manually if p is close to 100), then automatically less than half of elements in $[1, 100]$ are quadratic residues mod p, so p is not square-friendly.

Let $p = 109$. Then by direct computation

$$\left(\frac{102}{109}\right) = \left(\frac{104}{109}\right) = \left(\frac{105}{109}\right) = \left(\frac{106}{109}\right) = \left(\frac{108}{109}\right) = 1,$$

so 5 elements of $[101, 108]$ are quadratic residues mod p, so at most 49 elements of $[1, 100]$ are quadratic residues mod p.