Dalhousie University, MATH 3070
Midterm # 2 Solutions
Tuesday, November 4, 2008

1. (a) [10] *State Euler's Criterion and use it to prove that* -1 *is a quadratic residue modulo an odd prime* p *if and only if* $p \equiv 1 \pmod 4$.

   Euler's Criterion. Let p be an odd prime with $(a, p) = 1$. Then a is a quadratic residue mod p if and only if $a^{(p-1)/2} \equiv 1 \pmod p$.

   Plugging in $a = -1$ we see that it is a quadratic residue if and only if $(p-1)/2$ is even, which occurs if and only if $p \equiv 1 \pmod 4$.

   (b) [5] *Let* p *be an odd prime and* $(a, p) = 1$. *Prove that if* $p \equiv 3 \pmod 4$, *then the congruence* $x^4 \equiv a \pmod p$ *has either no solutions or exactly* 2 *solutions mod* p.

   Suppose $x^4 \equiv a \pmod p$ has a solution $x \equiv r \pmod p$. Then we may rewrite the congruence as $x^4 - r^4 \equiv 0 \pmod p$. Factoring, we find that $(x-r)(x+r)(x^2+r^2) \equiv 0 \pmod p$. So we have solutions $x \equiv \pm r \pmod p$ or $x^2 \equiv -r^2 \pmod p$. Note that $r \not\equiv -r \pmod p$ since p is odd, so we have at least two solutions. However, if $p \equiv 3 \pmod 4$, then -1 is a quadratic non-residue mod p. So $-r^2$ is also a quadratic non-residue mod p since r^2 is clearly a quadratic residue. Thus $x^2 \equiv -r^2 \pmod p$ has no solutions. Thus the only solutions to $x^4 \equiv r^4 \pmod p$ are $x \equiv \pm r \pmod p$.

2. [5] *Let* $n > 2$. *Prove that if* a *is a quadratic residue mod* n, *then* a *cannot be a primitive root mod* n.

   If $n > 2$ then either $n = 2^k, k \geq 2$ or n contains an odd prime factor. In either case, $\varphi(n)$ is even and so if $a \equiv r^2 \pmod n$ for some r, we find that $a^{\varphi(n)/2} \equiv r^{2\varphi(n)/2} \equiv r^{\varphi(n)} \equiv 1 \pmod n$. Thus $\mathrm{ord}_n(a) < \varphi(n)$, so a cannot be a primitive root mod n.

3. (a) [5] *Prove that* 3 *is a primitive root mod* 31.

   $\varphi(31) = 30$, so the possible orders of 3 are $1, 2, 3, 5, 6, 10, 15, 30$. Computing powers, we find that $3^1 = 3$, $3^2 = 9$, $3^3 = 27 \equiv -4$, $3^5 \equiv 9 \cdot -4 \equiv -36 \equiv -5$, $3^6 \equiv -15$, $3^{10} \equiv (3^5)^2 \equiv 25 \equiv -6$, and $3^{15} \equiv 3^{10}3^5 \equiv 30$. Since none of these are 1 mod 31, we find that the order of 3 mod 31 must be 30.

   (b) [5] *How many primitive roots are there mod* 961*?* ($961 = 31^2$)

   Since there is a primitive root mod 31, by problem 2 in homework 5 there must be a primitive root mod 31^2 (This primitive root is either 3 or 34). If there is at least one primitive root mod n, then there are exactly $\varphi(\varphi(n))$ primitive roots. Thus we have $\varphi(\varphi(31^2)) = \varphi(930) = \varphi(2)\varphi(3)\varphi(5)\varphi(31) = 1 \cdot 2 \cdot 4 \cdot 30 = 240$ primitive roots mod 961.

   (c) [5] *How many primitive roots are there mod* 899*?* ($899 = 900 - 1 = 29 \cdot 31$)

   By problem 2 in homework 5, composite numbers with at least two distinct odd factors have no primitive roots.

4. [5] *Let* p *be an odd prime. Prove that if* $p \equiv 1 \pmod 4$ *then exactly half of the quadratic residues* r *mod* p *lie in the interval* $1 \leq r \leq (p-1)/2$.

By problem 1a, if $p \equiv 1 \pmod 4$, then -1 is a quadratic residue mod p. Thus we find that $\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-a}{p}\right) = \left(\frac{-a}{p}\right)$. Thus a is a quadratic residue mod p if and only if $-a$ is. Therefore, the number of quadratic residues in the first half of the interval $[1, p-1]$ is the same as the number in the second half, and so exactly half of all the quadratic residues must lie in the interval $[1, (p-1)/2]$.

5. (a) [5] *Prove that for all $n > 1$, $\varphi(n)\sigma(n) < n^2$.*

Let $n = p_1^{a_1} \cdots p_k^{a_k}$ be its unique factorization. Then we find that

$$\begin{aligned}\varphi(n)\sigma(n) &= p_1^{a_1-1} \cdots p_k^{a_k-1}(p_1-1)\cdots(p_k-1) \times \left(\frac{p_1^{a_1+1}-1}{p_1-1}\right)\cdots\left(\frac{p_k^{a_k+1}-1}{p_k-1}\right) \\ &= p_1^{a_1-1} \cdots p_k^{a_k-1}(p_1^{a_1+1}-1)\cdots(p_k^{a_k+1}-1) \\ &< p_1^{a_1-1} \cdots p_1^{a_k-1}(p_1^{a_1+1} \cdots p_k^{a_k+1}) = p_1^{2a_1} \cdots p_k^{2a_k} = n^2.\end{aligned}$$

(b) [5] *Let p be an odd prime. Prove that $\varphi(p-1) < p/2$.*

Solution 1: If p is an odd prime then there are exactly $\varphi(p-1)$ primitive roots mod p. But by problem 2, none of these are quadratic residues. So they must be some subset of the $(p-1)/2$ quadratic non-residues mod p. Thus $\varphi(p-1) \leq (p-1)/2 < p/2$.

Solution 2: If p is an odd prime then $p-1$ is even. Thus none of the $(p-1)/2$ even numbers in the interval $[1, p-1]$ are coprime to $p-1$. Therefore $\varphi(p-1) \leq (p-1)/2 < p/2$.

6. (a) [5] *State the Law of Quadratic Reciprocity.*

Let p and q be distinct odd primes. Then the product of Legendre symbols

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}.$$

(b) [5] *Determine whether 33 is a quadratic residue mod 43.*

We need to calculate $\left(\frac{33}{43}\right) = \left(\frac{3}{43}\right)\left(\frac{11}{43}\right)$. Applying quadratic reciprocity we find that

$$\left(\frac{3}{43}\right)\left(\frac{11}{43}\right) = (-1)^{21\cdot 1}\left(\frac{43}{3}\right)(-1)^{21\cdot 5}\left(\frac{43}{11}\right) = \left(\frac{1}{3}\right)\left(\frac{-1}{11}\right) = 1 \cdot -1 = -1.$$

So 33 is a quadratic non-residue mod 43.

7. [5] *Let $n > 2$. Consider the statement, "For all a coprime to n, $\gcd(\mathrm{ord}_n(a), \varphi(n)) > 1$." Either give a proof of this statement, or characterize all the values of a for which it fails, and prove it for all the remaining values of a.*

Note that for all a coprime to n, $\mathrm{ord}_n(a) \mid \varphi(n)$ so $\gcd(\mathrm{ord}_n(a), \varphi(n)) = \mathrm{ord}_n(a)$. This is greater than 1 if and only if $\mathrm{ord}_n(a) > 1$. So the statement is false unless we impose the condition that $\mathrm{ord}_n(a) > 1$, or equivalently, $a \not\equiv 1 \pmod n$.