Math 4150-B, Intro to Number Theory
EXAM 2 Solutions

1. Show that if $F_n = 2^{2^n} + 1$, the n-th Fermat number, is a prime, then every quadratic non-residue modulo F_n is a primitive root (Hint: How many primitive roots, quadratic non-residues are there?).

   Solution:

   There are $(F_n - 1)/2$ quadratic non-residues modulo F_n. Moreover, since there is a primitive root modulo F_n (its a prime), there are $\varphi(\varphi(F_n)) = \varphi(2^{2^n}) = 2^{2^n-1}(2-1) = 2^{2^n-1} = (F_n - 1)/2$ primitive roots. Furthermore, every primitive root is a quadratic non-residue, as if $r \equiv x^2$, then $r^{(F_n-1)/2} \equiv x^{F_n-1} \equiv 1$ by Euler's Theorem, contradicting that r is a primitive root. Thus, the sets of primitive roots and quadratic non-residues are the same, as one contains the other and they have the same size.

2. (a) Suppose that r is a primitive root modulo an odd prime p. Show that

   $$(p-1)! \equiv r^{\frac{p(p-1)}{2}} \pmod p$$

   (Hint: Note that $(p-1)! \pmod p$ is a product of one representative from each of the different invertible congruence classes modulo p.)

   (b) Use part (a) directly to give a proof of Wilson's Theorem for odd primes p, namely, that

   $$(p-1)! \equiv -1 \pmod p.$$

   Solution:

   (a) Following the hint, and noting that the powers $r^1, r^2, \ldots, r^{p-1}$ hit all the invertible residue classes modulo p (since r is a primitive root), we see that $(p-1)!$ is congruent modulo p to $r^1 \cdot r^2 \cdot \ldots \cdot r^{p-1} = r^{1+2+\ldots+(p-1)} = r^{p(p-1)/2}$.

   (b) Since $a = r^{(p-1)/2}$ has square congruent to $r^{p-1} \equiv 1 \pmod p$, we have $a^2 \equiv 1 \pmod p$. As we've proven in class (and can deduce from the facts that $a^2 - 1 = (a+1)(a-1)$ and that a product of numbers is 0 modulo a prime if and only if one of the factors is), we know that $a \equiv \pm 1 \pmod p$. But taking r to be a primitive root (which we know exists modulo any prime), we know that in this case a isn't congruent to 1, or else the order of r would be too small. Thus, in the situation of (a), since p is odd, we have $(p-1)! \equiv a^p \equiv (-1)^p \equiv -1 \pmod p$.

3. The number $p = 65,537 = 2^{2^4} + 1$ is a Fermat prime. Use problem 1 above to show that 3 is a primitive root modulo p.

   Solution: By problem 1, it suffices to show that 3 is a quadratic non-residuel By quadratic reciprocity (note: $p \equiv 1 \pmod 4$ and $p \equiv (-1)^{16} + 1 \equiv 2 \pmod 3$), $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$ (the last symbols is -1 as $1^2 \equiv 2^2 \equiv 1 \pmod 3$), as desired.

4. Suppose that a function $f(n)$ is a multiplicative function with summatory function $\sum_{d|n} f(d) = n\sigma_0(n)$, where $\sigma_0(n) = \sum_{d|n} 1$ is the number of divisors of n. Use Möbius inversion to compute $f(100)$.

   Solution: Möbius inversion tells us that

$$f(n) = \sum_{d|n} \mu(d) \cdot \sigma_0(n/d) \cdot (n/d).$$

   The divisors of 100 are $1, 2, 4, 5, 10, 20, 25, 50$, and 100. The μ values of these numbers are, respectively, $1, -1, 0, -1, 1, 0, 0, 0, 0$, the complementary divisors n/d are, respectively, $100, 50, 25, 20, 10, 5, 4, 2, 1$. Thus, $f(100) = \sigma_0(100) \cdot 100 - \sigma_0(50) \cdot 50 - \sigma_0(20) \cdot 20 + \sigma_0(10) \cdot 10 = 900 - 300 - 120 + 40 = 520$.

5. (a) Suppose that r is a primitive root modulo an odd prime p. Find the index $\text{ind}_r(-1)$.

   (b) It turns out that 13 is a primitive root modulo the prime 479. Use this information, and part (a), to determine whether $x^4 \equiv -13 \pmod{479}$ has a solution (you don't need to compute this solution). If it has a solution, determine how many incongruent solutions it has.

   Solution:

   (a) As in problem 2, $r^{(p-1)/2}$ is a number which isn't 1 mod p but whose square is, and hence $r^{(p-1)/2} \equiv -1 \pmod{p}$. Thus, the index of -1 is $(p-1)/2$.

   (b) Taking indices of both sides, this equation reduces to $4 \cdot \text{ind}_{13}(x) \equiv \text{ind}_{13}(-1) + \text{ind}_{13}(13) \equiv (p-1)/2 + 1 \equiv (p+1)/2 = 240 \pmod{478}$. This linear congruence has a solution, in fact 2 solutions, as $(4, 478) = 2|240$.