MATH 115, SUMMER 2012
WORKSHEET FOR LECTURE 14

JAMES MCIVOR

(1) (8 points) Find all solutions to the congruence $x^2 - 4x + 23 \equiv 0 \mod 125$.

Solution: Working mod 5, we get the solutions $x = 1$, $x = 3$. These are both nonsingular, since $f'(x) = 2x - 4$, so $f'(1) = -2$, $f'(3) = 2$, and both are nonzero mod 5.

Now let $a = 1$. $f'(a)^{-1} = 2$, so

$$a_2 = 1 - f(1) \cdot 2 = 1 - 40 = -39 \equiv 11 \mod 25,$$
$$a_3 = 11 - f(11) \cdot 2 = 11 - 100 \cdot 2 \equiv 61 \mod 125$$

Next let $a = 3$; then $f'(3)^{-1} = 3$, so

$$a_2 = 3 - f(3) \cdot 3 = 3 - 20 \cdot 3 = -57 \equiv -7 \mod 25$$
$$a_3 = -7 - f(-7) \cdot 3 = -7 - 100 \cdot 3 = -307 \equiv -57 \equiv 68 \mod 125$$

Thus the two solutions mod 125 are 61 and 68.

(2) (3 points) Let a be a unit in the ring $\mathbb{Z}/14$. What are all the possible values of the order of a?

Solution: Any unit has an order that divides $\phi(14) = 6$, so the possible orders are 1,2,3,6.

(3) (2 points) Let $m > 1$. Suppose that $m - 1$ is a primtive root mod m. What are the possible values of m?

Solution: Since $m - 1 \equiv -1 \mod m$, and $m - 1$ is a primitive root, the set of powers of $m - 1$, which is congruent to the set $\{-1, 1\}$, forms a reduced residue system. If $m = 2$, then $1 = -1$, so this set has size one, hence $m = 2$. Otherwise $\phi(m) = 2$. What numbers m have $\phi(m) = 2$? If $m > 2$ is prime, $\phi(m) = m - 1 = 2$ implies $m = 3$. If m is composite, its only prime factors can be 2 or 3, by the multiplicative property of ϕ. Thus $m = 2^\alpha 3^\beta$.

(4) (2 points) Find the order of the element 2 in $\mathbb{Z}/19$.

Solution: The possile orders are divisors of $\phi(19) = 18$, namely 1,2,3,6,9,18. We just need to compute 2 to each of these powers, and not the first time we get 1 mod 19. First we compute some powers of 2 mod 19:

$$2^0 = 1, 2^1 = 2, 2^2 = 4, 2^4 = 16, 2^8 \equiv 9 \mod 19$$

We can use just these to compute the other powers of 2 we're interested in:

$$2^3 = 2^2 \cdot 2^1 = 4 \cdot 2 = 8, 2^6 = (2^3)^2 = 8^2 = 64 \equiv 7, 2^9 = 2^8 \cdot 2 \equiv 9 \cdot 2 = 18 = -1$$

Once we see -1 in this list, we're done - since $2^9 \equiv -1$, $2^18 \equiv 1$. Of course, since none of the powers 1,2,3,6,9 worked, the only one left was 18 anyway. So 2 is actually a primitive root mod 19.

Quadratic Residues Practice:

(1) Determine whether 3 is a QR or a QNR mod p for the following values of p: 11,13,17,19.

We don't have any tricks (yet) to deal with large primes, so it's most efficient to first make a list of the squares up to 18^2:

$$0, 1, 2, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256, 289, 324.$$

Now subtract 3 from each:

$$-3, -2, 1, 6, 13, 22, 33, 46, 61, 78, 97, 118, 141, 166, 193, 222, 253, 286, 321$$

Now we just reduce these mod 11,13,17,19 and see whether we get any zeroes.

- mod 11, we see $22 \equiv 0$, so 3 is a QR mod 11.
- mod 13, $78 \equiv 0$, so 3 is a QR mod 13
- mod 17, none of these are zero, so 3 is a QNR mod 17
- mod 19, none of these are zero, so 3 is a QNR mod 19

(2) Evaluate the following Legendre symbols:

(a) $\left(\frac{2}{5}\right) = -1$
(b) $\left(\frac{3}{5}\right) = -1$
(c) $\left(\frac{6}{5}\right) = \left(\frac{2}{5}\right)\left(\frac{3}{5}\right) = (-1)(-1) = 1$
(d) $\left(\frac{432}{5}\right) = \left(\frac{2}{5}\right) = -1$
(e) $\left(\frac{80}{5}\right) = 0$ since $5|80$.
(f) $\left(\frac{-1}{19}\right) = -1$ since $19 \equiv 3 \mod 4$.
(g) $\left(\frac{4}{7}\right) = 1$ (four is always a quadratic residue mod any $p > 3$).
(h) $\left(\frac{8}{3}\right) = \left(\frac{2}{3}\right) = -1$.

(3) Prove the "other useful properties of the Legendre symbol" listed in lecture following the key fact: $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$.

Solution: For example, to see that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, just compute

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

and since this number can only be ± 1, and $p > 2$, congruence mod p implies equality.