Math 115, Summer 2012
Homework 4
Solution

NZM a.b.c refers to a problem in our text, 5th edition - these may differ slightly from the problems appearing in other editions, so use the version printed here to be safe).

(1) (NZM 3.1.7) Which of the following congruences have solutions?
(a) $x^2 \equiv 2 \mod 61$
(b) $x^2 \equiv -2 \mod 61$
(c) $x^2 \equiv 2 \mod 59$
(d) $x^2 \equiv -2 \mod 118$

Solution: Only (d) has a solution. To figure out (d), split the congruence into the two congruences

$$x^2 \equiv -2 \mod 59$$
$$x^2 \equiv -2 \equiv 0 \mod 2$$

The second one just say that x must be even, so we'll be done if we can find a solution to the first one that is even. You can use Euler's criterion to find that there are exactly two solutions to the first one. Let x_0 be one of them, and by reducing mod 59 we can assume $0 < x_0 < 59$. Now if x is a solution, then so is $-x$ (mod 59), and by reducing $-x_0$ so it's in the range $(0, 59)$, we can write $-x_0 = 59 - x_0$. Therefore if x_0 is even, then $-x_0$ is odd, and vice versa, so exactly one of the two solutions is even, and this even solution solves both congruences, hence it solves the original congruence.

(2) (NZM 3.1.13) Prove that if r is a quadratic residue mod $m > 2$, then $r^{\phi(m)/2} \equiv 1 \mod m$.

Solution: By the assumption, there is x such that $x^2 \equiv r \mod p$. Raising both sides to the power $\phi(m)/2$ gives

$$x^{\phi(m)} \equiv r^{\phi(m)/2} \mod m$$

Now by definition of quadratic residue, r is prime to m, and hence so is x. Thus by Euler's Theorem, $x^{\phi(m)} \equiv 1 \mod m$, and we're done.

(3) (NZM 3.1.19) Prove that for all primes p, $x^8 \equiv 16 \mod p$ has a solution. [Hint in the book]

Solution: First, if $p = 2$, we get $x^8 \equiv 0 \mod 2$, for which any even x is a solution. Now let $p > 2$. For this, following the hint, we need a formula which I didn't give in class. Sorry if this caused confusion. Thm 2.37 is a sort of generalized Euler's Criterion, which says in this case that

$$x^8 \equiv 16 \mod p$$

has solutions for x if and only if

$$16^{\frac{p-1}{(8,p-1)}} \equiv 1 \mod p,$$

which can be rewritten as

$$2^{4\frac{p-1}{(4,p-1)}} \equiv 1 \mod p$$

Now $g = (8, p-1)$ can only be $g = 1, 2, 4$, or 8. If $g < 8$, then $4/g$ is an integer, and we have

$$(2^{p-1})^{4/g} \equiv 1^{4/g} \equiv 1 \mod p$$

by Euler's Theorem. Thus our congruence has a solution except possibly when $(8, p-1) = 8$. In this case, we have $p \equiv 1 \mod 8$, which tells us that $\left(\frac{2}{q}\right) = 1$, so the congruence $x^2 \equiv 2 \mod p$ has a solution. Raising both sides to the fourth power shows that $x^8 \equiv 16 \mod p$, has a solution.

(4) (NZM 3.2.3) Prove that if a prime p has the form $4k+1$, and is a quadratic residue mod an odd prime q, then q is a quadratic residue mod p.

Solution:

$$1 = \left(\frac{4k+1}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{4k}{2}\frac{q-1}{2}} = \left(\frac{q}{p}\right),$$

so q is a QR mod p.

(5) (NZM 3.2.4) Which of the following congruences is solvable?

(a) $x^2 \equiv 5 \mod 227$
(b) $x^2 \equiv 5 \mod 229$
(c) $x^2 \equiv -5 \mod 227$
(d) $x^2 \equiv -5 \mod 229$
(e) $x^2 \equiv 7 \mod 1009$
(f) $x^2 \equiv -7 \mod 1009$

[Hint: 227,229, and 1009 are primes]

Solution: b,c,d,e,f

(6) (NZM 3.2.6) Decide whether $x^2 \equiv 150 \mod 1009$ is solvable or not.

Solution: Note that 1009 is prime (look it up!)

$$\left(\frac{150}{1009}\right) = \left(\frac{2}{1009}\right)\left(\frac{3}{1009}\right)\left(\frac{5}{1009}\right)^2 = 1 \cdot \left(\frac{1009}{3}\right)(-1)^{\frac{1008}{2}\frac{2}{2}} \cdot 1 = 1 \cdot 1 \cdot 1 = 1,$$

so it has a solution.

(7) (NZM 3.2.7) Find all primes such that $x^2 \equiv 13 \mod p$ has a solution.

Solution: If $p = 2$, we have the solution $x = 1$. For any odd p, let p' denote its least positive residue mod 13. Then

$$\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right) = \left(\frac{p'}{13}\right),$$

so p' must be a QR mod 13. A quick check shows that $p' \equiv \pm 1, \pm 3, \pm 4 \mod 13$.

(8) (NZM 3.2.9) Find all primes q such that $\left(\frac{5}{q}\right) = -1$.

Solution: First suppose $q = 2$. The congruence $x^2 \equiv 5 \equiv 1 \mod 2$ has a solution, so this value of q does not work. Now let q be odd, and as above, let q' be the least positive residue of q mod 5; then

$$\left(\frac{5}{q}\right) = \left(\frac{q}{5}\right) = -1$$

implies that q' is a QNR mod 5, so it must be either 2 or 3. Hence the allowed values of q are those odd primes q for which $q \equiv 2, 3 \mod 5$.

(9) (NZM 3.2.13) Prove that there are infinitely many primes of the form $3n+1$.

[Hint: Proceed just like in Euclid's proof that there are infinitely many primes, namely assume there are only finitely many, say $p_1, \dots, p_r$. We want a contradiction. Let $a = p_1 \cdots p_r$ be their product. Note a has the form $3n+1$, too. Here's the trick: Look at $N = (2a)^2 + 3$. Now consider a prime q dividing n, and show it cannot be in our list $p_1, \dots, p_r$, using quadratic reciprocity. Note the factor of 2 in the expression for N is to make sure that q is odd.]

Solution: Suppose there are finitely many such, call them $p_1, \dots, p_r$. Set $a = p_1 \cdots p_r$, note that a also has the form $3n+1$ and let $N = (2a)^2 + 3$. Let q be a prime with $q|N$, so q is odd. First we show q can't be one of the p_is. Since $a \equiv 0 \mod p_i$, $N \equiv 3 \mod p_i$ for each i. But since $q|N$, $N \equiv 0 \mod q$, so q is different from the p_is (note none of the p_is are 3, since they all have the form $3n+1$). Next, we have from the definition of N that

$$(2a)^2 \equiv -3 \mod q$$

In particular, the congruence $x^2 \equiv -3 \mod q$ has a solution in x. So $\left(\frac{-3}{q}\right) = 1$.

But we can also compute $\left(\frac{-3}{q}\right)$ with quadratic reciprocity:

$$\left(\frac{-3}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{3}{q}\right) = (-1)^{\frac{q-1}{2}}\left(\frac{q}{3}\right)(-1)^{\frac{3-1}{2}\frac{q-1}{2}} = \left(\frac{q}{3}\right),$$

and $\left(\frac{q}{3}\right) = 1$ iff $q \equiv 1$ mod 3, since $\left(\frac{q}{3}\right) \equiv (q)^{\frac{3-1}{2}} \equiv q \mod 3$. We saw above that $\left(\frac{-3}{q}\right) = 1$, and therefore we have shown that $q \equiv 1 mod 3$, so q is a prime of the form $3n+1$, which is a contradiction, since we checked above that q is different from the p_is, and we assumed that those were all of the primes of the form $3n+1$.

(10) (NZM 3.2.14) Let p and q be twin primes, that is, primes satisfying $q = p+2$. Prove that there is an integer a such that $p|(a^2 - q)$ if and only if there is an integer b such that $q|(b^2 - p)$.

Solution: There exists an integer a such that $p|(a^2 - q)$ iff $a^2 \equiv q \mod p$ has a solution iff

$$\left(\frac{q}{p}\right) = 1$$

Similarly, there exists a b such that $q|(b^2 - q)$ iff

$$\left(\frac{p}{q}\right) = 1,$$

so it will be enough to show the two Legendre symbols are the same. But by quadratic reciprocity,

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

and the exponent on the last -1 is even, since $\frac{p-1}{2}$ and $\frac{p+1}{2}$ are adjacent integers, so one of them must be even.