Midterm 2 Review

Tim Smits

1. (a) Solve the system of congruence equations:

$$\begin{cases} x \equiv 3 \bmod 5 \\ x \equiv 1 \bmod 7 \\ x \equiv 6 \bmod 8 \end{cases}$$

   (b) Solve $x^5 \equiv 7 \bmod 72$.

   (c) Does $x^2 - 3x + 64 \equiv 0 \bmod 113$ have a solution?

   (d) Find all primes p such that $\left(\frac{10}{p}\right) = 1$.

2. Let $f(x)$ be a polynomial with integer coefficients, and let m, n be relatively prime integers.

   (a) Prove that $f(x) \equiv 0 \bmod mn$ has a solution if and only if $f(x) \equiv 0 \bmod m$ and $f(x) \equiv 0 \bmod n$ both have a solution.

   (b) Let N_1 be the number of solutions to $f(x) \equiv 0 \bmod m$ and N_2 be the number of solutions to $f(x) \equiv 0 \bmod n$. Prove that the number of solutions to $f(x) \equiv 0 \bmod mn$ is $N = N_1 N_2$.

   (c) Compute the number of solutions to $x^2 \equiv 1 \bmod 2^4 \cdot 3^3 \cdot 5^2 \cdot 7$.

3. Use the line passing through $(3, 2)$ to parametrize all rational points on the hyperbola $x^2 - 2y^2 = 1$.

4. (a) Show that a positive integer n is perfect if and only if $\sum_{d|n} \frac{1}{d} = 2$. (Here the sum is taken over all divisors d of n).

   (b) If n is perfect, show that kn is not perfect for $k > 1$.

5. Let $p \equiv 1 \bmod 4$ be a prime.

   (a) Prove that the sum of quadratic residues $a \bmod p$ with $1 \leq a \leq p-1$ is $\frac{p(p-1)}{4}$.

   (b) Prove that $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a = 0$.

6. A *Fermat prime* is a prime p with $p = 2^{2^n} + 1$ for some $n \geq 1$. Prove that if p is a Fermat prime, then $3^{(p-1)/2} \equiv -1 \bmod p$. (This can be used to show that $2^{2^{14}} + 1$ is composite, although we don't know any of it's prime factors!)

Hints

2. Show that if $f(x_1) \equiv 0 \bmod m$ and $f(x_2) \equiv 0 \bmod n$ then the solution to $\begin{cases} x \equiv x_1 \bmod m \\ x \equiv x_2 \bmod n \end{cases}$ satisfies $f(x) \equiv 0 \bmod mn$.

5a. If a is a quadratic residue, what does this mean about $p - a$?

5b. Notice that $\left(\frac{a}{p}\right) a = a$ if a is a square mod p and is $-a$ otherwise.

6. Rewrite the congruence as a statement about a certain Legendre symbol.

Solutions

1. (a) We use the Chinese remainder theorem. Since $x \equiv 3 \bmod 5$, write $x = 3+5k$ for some k. This says $3+5k \equiv 1 \bmod 7$, so $5k \equiv 5 \bmod 7$. This says $k \equiv 1 \bmod 7$, so $k = 1+7m$ for some m. Plugging in says $x = 3+5(1+7m) = 8+35m$. Plugging into the last equation, $8+35m \equiv 6 \bmod 8$ so $3m \equiv 6 \bmod 8$. This says $m \equiv 2 \bmod 8$, so $m = 2+8\ell$. for some ℓ. Plugging in gives $x = 8+35(2+8\ell) = 78+280\ell$, so the solution is $x \equiv 78 \bmod 280$.

   (b) We have $\varphi(72) = \varphi(8 \cdot 9) = \varphi(8)\varphi(9) = 4 \cdot 6 = 24$. We now wish to find d such that $5d \equiv 1 \bmod 24$. By inspection, we see that $d = 5$ works. Exponentiating and using Euler's theorem, we have $x \equiv x^{25} \equiv (x^5)^5 \equiv 7^5 \equiv 31 \bmod 72$.

   (c) Completing the square, the quadratic is $(x-\frac{3}{2})^2 + \frac{247}{4}$. In order to make sure all coefficients are integers, multiply by 4 to obtain $(2x-3)^2 + 247$. Since 4 is invertible mod 113, asking if $x^2 - 3x + 64$ has a solution mod 113 is the same as asking if $(2x-3)^2 + 247 \bmod 113$ has a solution. Equivalently, does $(2x-3)^2 \equiv -21 \bmod 113$ have a solution? We have $\left(\frac{-21}{113}\right) = \left(\frac{-1}{113}\right)\left(\frac{3}{113}\right)\left(\frac{7}{113}\right)$. Note that $113 \equiv 1 \bmod 4$ and is prime, so we can use quadratic reciprocity to compute the last two Legendre symbols. We have $\left(\frac{3}{113}\right) = \left(\frac{113}{3}\right) = \left(\frac{2}{3}\right) = -1$, and $\left(\frac{7}{113}\right) = \left(\frac{113}{7}\right) = \left(\frac{1}{7}\right) = 1$. We also have $\left(\frac{-1}{113}\right) = 1$, so $\left(\frac{-21}{113}\right) = -1$. This says there are no solutions to the quadratic congruence.

   (d) We have $\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right)$, so we want either both Legendre symbols to be 1 or both to be -1. Note that if $p = 2, 5$ that $10 \equiv 0 \bmod p$. If $p \neq 2, 5$, then by quadratic reciprocity, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. The squares mod 5 are $1, 4$ and the non-squares are $2, 3$ so $\left(\frac{5}{p}\right) = \begin{cases} 1 & p \equiv 1, 4 \bmod 5 \\ -1 & p \equiv 2, 3 \bmod 5 \end{cases}$. We also know that $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1, 7 \bmod 8 \\ -1 & p \equiv 3, 5 \bmod 8 \end{cases}$. Using the Chinese remainder theorem to solve the various systems of congruences gives $p \equiv 1, 3, 9, 13, 27, 31, 37, 39 \bmod 40$ as the 8 congruence classes of primes that work.

2. (a) First, suppose that $f(x) \equiv 0 \bmod mn$ has a solution, say c. Then $f(c) \equiv 0 \bmod mn$ says $f(c) \equiv 0 \bmod m$ and $f(c) \equiv 0 \bmod n$ so c is a solution to both $f(x) \equiv 0 \bmod m$ and $f(x) \equiv 0 \bmod n$. Conversely, suppose that $f(x_1) \equiv 0 \bmod m$ and $f(x_2) \equiv 0 \bmod n$. for some x_1, x_2. By the Chinese remainder theorem, there is an integer y such that $y \equiv x_1 \bmod m$ and $y \equiv x_2 \bmod n$. Thus, $f(y) \equiv f(x_1) \equiv 0 \bmod m$ and $f(y) \equiv f(x_2) \equiv 0 \bmod n$. As m and n are relatively prime, this says $mn \mid f(y)$, i.e. $f(y) \equiv 0 \bmod mn$ as desired.

   (b) Part (a) says that each pair of solutions (x_1, x_2) to the congruence equations $f(x) \equiv 0 \bmod m$ and $f(x) \equiv 0 \bmod n$ gives rise to a solution mod mn, and the Chinese remainder theorem says such a solution is *unique*. Therefore, counting the number of solutions to $f(x) \equiv 0 \bmod mn$ is the same as counting the number of pairs (x_1, x_2), which by definition, is $N_1 N_2$.

   (c) By the previous part, the number of solutions can be found by computing the number of solutions to each of $x^2 \equiv 1 \bmod m$, where $m = 7, 16, 25, 27$. Note that $x^2 \equiv 1 \bmod 16$ has 4 solutions, and each of $x^2 \equiv 1 \bmod 7, 25, 27$ have 2 solutions by midterm 1 review problem 6. This gives a total of $4 \cdot 2 \cdot 2 \cdot 2 = 32$ solutions.

3. Let (p, q) be a point on our curve, and consider the line of slope $m = \frac{q-2}{p-3}$ passing through (p, q) and $(3, 2)$. The equation of this line is $y = 2+m(x-3)$, so plugging into the equation says $x^2 - 2(2+m(x-3))^2 = 1$. Grouping and dividing by the coefficient on x^2 gives $x^2 + \frac{4m(3m-2)}{1-2m^2}x - \frac{3(6m^2-8m+3)}{1-2m^2} = 0$. Since (p, q) and $(3, 2)$ are rational points, we know that p and 3 are roots of this quadratic. The constant term is the product of the roots, so $3p = -\frac{3(6m^2-8m+3)}{1-2m^2}$, so $p = \frac{6m^2-8m+3}{2m^2-1}$. We have $q = 2 + m(p-3) = \frac{-2(2m^2-3m+1)}{2m^2-1}$. We have shown that any point (p, q) on the curve can be written in terms of the slope of the line connecting it to the point $(3, 2)$ (when such a slope is well-defined). A rational point has a rational slope m, and given any rational number m the point produced above has rational coordinates. The only points

our method miss are when the slope is not-well defined, i.e. the vertical line $x = 3$. Solving $9 - 2y^2 = 1$ says $y = \pm 2$, so the only point we have missed is $(3, -2)$. Therefore any rational point is either $(3, -2)$ or $(\frac{6m^2-8m+3}{2m^2-1}, \frac{-2(2m^2-3m+1)}{2m^2-1})$ for $m \in \mathbb{Q}$.

4. (a) An integer n is perfect if and only if $\sigma(n) = 2n$, or equivalently, if $\frac{\sigma(n)}{n} = 2$. Write $\sigma(n) = \sum_{d|n} d$, so $\frac{\sigma(n)}{n} = \sum_{d|n} \frac{d}{n}$. Since d is a divisor of n, we have $n = dd'$ for some other divisor d'. Therefore, $\frac{d}{n} = \frac{1}{d'}$. Taking the sum over all divisors d will produce all possible choices of d', so $\sum_{d|n} \frac{d}{n} = \sum_{d'|n} \frac{1}{d'}$. Therefore, n is perfect if and only if $\sum_{d|n} \frac{1}{d} = 2$.

   (b) If $d \mid n$, then $kd \mid kn$ for any $k > 1$. Therefore, $\sum_{d|kn} \frac{1}{d} = \sum_{d|n} \frac{kd}{kn} + \text{stuff} = \sum_{d'|n} \frac{1}{d'} + \text{stuff} > 2$ since n is perfect. By part (a), this means kn is not perfect.

5. (a) Since $p \equiv 1 \bmod 4$, -1 is a square mod p. Therefore, if a is a square mod p, then so is $p - a$. The pair $(a, p - a)$ sums up to p, so we just need to count how many such pairs there are. We know there are $\frac{p-1}{2}$ quadratic residues between 1 and $p - 1$, so there are $\frac{p-1}{4}$ such pairs. This says the sum is $\frac{p(p-1)}{4}$ as desired.

   (b) We can write $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a = \sum_{a \equiv \square \bmod p} a - \sum_{a \not\equiv \square \bmod p} a$. By the same argument as part (a), if a is a non-square mod p then so is $p - a$ because -1 is a square mod p. Therefore, both sums are $\frac{p(p-1)}{4}$, and so cancel out. Thus, $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a = 0$ as desired.

6. By Euler's criterion, $3^{(p-1)/2} \equiv \left(\frac{3}{p}\right) \bmod p$. Therefore, we wish to show that $\left(\frac{3}{p}\right) = -1$. Note that $p \equiv 1 \bmod 4$, so by quadratic reciprocity, we wish to show that $\left(\frac{p}{3}\right) = -1$. Also notice that $p \equiv (-1)^{2^n} + 1 \equiv 2 \bmod 3$, and 2 is not a square mod 3. This proves what we wanted.