CLASS 12, GIVEN ON 10/18/2010, FOR MATH 25

1. Polynomial congruences

We now have a good understanding of how to solve systems of linear congruences to different moduli, regardless of whether they are mutually coprime or not. In the case of mutually coprime moduli, the CRT provides the answer for how solutions of simultaneous systems are assembled from solutions to the individual congruences. In the case of moduli which are powers of the same prime, we have a compatibility requirement which must be satisfied for there to be a simultaneous solution.

We will now briefly consider the case of what happens when we have congruence equations which are polynomial of degree higher than one. In general, this is a difficult problem, but we will be able to make a few elementary observations.

Let $f(x)$ be a polynomial with integer coefficients. We want to solve $f(x) \equiv 0 \mod n$. Of course, given a particular $f(x)$, one can solve this problem by trying each of the n possibilities for x. However, there is no easy criterion like that which exists for linear congruences to easily test whether such a polynomial congruence has solutions or not (and if so, how many there are, and how to easily describe them).

However, the first observation is that there are always finitely many solutions (at most n), and therefore the single equation $f(x) \equiv 0 \mod n$ is equivalent to determining whether one in a set of linear congruences is true.

Examples.

- Consider the congruence $x^2 \equiv 1 \mod 7$. This has the two solutions $x \equiv 1, 6 \mod 7$. Therefore, the original congruence is equivalent to asking whether either $x \equiv 1 \mod 7$ or $x \equiv 6 \mod 7$ is true.
- Simultaneously solve the pair of congruences $x^2 \equiv 1 \mod 5, x \equiv 2 \mod 4$. Although the first congruence is not linear, we can reduce it to asking whether a set of linear congruences is true. In particular, $x^2 \equiv 1 \mod 5$ if and only if $x \equiv 1, 4 \mod 5$. Therefore, we want to determine when either $x \equiv 1 \mod 5$ or $x \equiv 4 \mod 5$, and also when $x \equiv 2 \mod 4$.

  This breaks down the original problem into solving two different systems of linear congruences. The system $x \equiv 1 \mod 5, x \equiv 2 \mod 4$ is solved by $x \equiv 6 \mod 20$, while the system $x \equiv 4 \mod 5, x \equiv 2 \mod 4$ is solved by $x \equiv 14 \mod 20$. Therefore, the original system has solutions $x \equiv 6, 14 \mod 20$.
- More generally, if you are asked to simultaneously solve a system of congruences, not necessarily linear, a general approach to this problem is to break down each congruence into the list of linear congruences it is equivalent to. One then needs to solve many different systems of linear congruences, equal to the product of the number of linear congruences in each list.

  For instance, if we find that $f(x) \equiv 0 \mod n_1$ has N_1 solutions mod n_1, while $g(x) \equiv 0 \mod n_2$ has N_2 solutions mod n_2, then we need to solve $N_1 N_2$ different pairs of linear congruences.

A special case of the above is the following proposition:

Proposition 1 (Theorem 3.11)**.** *Let $n_1, \ldots, n_k$ be a mutually coprime set of positive numbers. Let $n = n_1 \ldots n_k$. If $f(x) \equiv 0 \mod n_i$ has N_i solutions mod n_i, then $f(x) \equiv 0 \mod n$ has $N_1 \ldots N_k$ solutions mod n.*

Proof. If $f(x) \equiv 0 \mod n$, then $f(x) \equiv 0 \mod n_i$ for each i, since $n_i | n$. In particular, each solution $x \mod n$ induces a k-tuple of solutions $x \mod n_i$ to the k congruences $f(x) \equiv 0 \mod n_i$. Conversely, given a k-tuple of solutions $a_1, \ldots a_k$ to $f(x) \equiv 0 \mod n_i$, we can find a unique $a \mod n$ such that $a \equiv a_i \mod n_i$, by the CRT. (We are simultaneously solving the system $x \equiv a_i \mod n_i$.) In particular, $f(a) \equiv 0 \mod n_i$; therefore, $a \mod n$ is a solution to $f(x) \equiv 0 \mod n$. This means that each k-tuple of solutions to $f(x) \equiv 0 \mod n_i$ induces a solution to $f(x) \equiv 0 \mod n$. One easily sees that these two associations are inverse to each other, so there is a 1-1 correspondence between solutions to $f(x) \equiv 0 \mod n$ and simultaneous solutions to $f(x) \equiv 0 \mod n_i$.

Since each $f(x) \equiv 0 \mod n_i$ has N_i solutions, altogether there are $N_1 \ldots N_k$ possible different k-tuples of solutions to these congruences, and therefore $N_1 \ldots N_k$ different solutions mod n to $f(x) \equiv 0 \mod n$. □

An interesting application of this proposition is to the question of when $x^2 \equiv 1 \mod n$ has exactly 2 solutions mod n. Recall that $x^2 \equiv 1 \mod 8$ has four solutions mod 8, so it is possible for this equation to have more than two solutions. Contrast this to the situation for the equation $x^2 - 1 = 0$, when considered as an equation over real or complex numbers, where there are exactly two solutions.

Proposition 2 (Example 3.18)**.** *Let n have k distinct prime divisors. If n is odd, then $x^2 \equiv 1 \mod n$ has 2^k solutions. If $2|n$, but $4 \nmid n$ (equivalently, $2||n$), then there are 2^{k-1} solutions. If $4||n$, then there are 2^k solutions, and if $8|n$, then there are 2^{k+1} solutions.*

Proof. By the previous proposition, we can reduce this question to asking how many solutions $x^2 \equiv 1 \mod n$ has when n is a prime power. Let us first consider the case where n is odd; ie, $n = p^e$ for p and odd prime. The equation $x^2 \equiv 1 \mod p^e$ is equivalent to $p^e \mid (x^2 - 1) = (x-1)(x+1)$. In particular, $p \mid (x-1)(x+1)$. But this means that either $p \mid (x-1)$ or $p \mid (x+1)$; ie, $x \equiv 1, -1 \mod p$. As a matter of fact, if $p^e \mid (x-1)(x+1)$, we must have $p^e \mid (x-1)$ or $p^e \mid (x+1)$, because if $p \mid (x-1)$, then $p \nmid (x+1) = (x-1) + 2$, since $p > 2$, and similarly if $p \mid (x+1)$. So the only possible solutions to $x^2 \equiv 1 \mod p^e$ are $x \equiv 1, -1 \mod p^e$, and it is clear that these are both distinct solutions.

Now consider what happens when $n = 2^e$. If $n = 2$, then $x^2 \equiv 1 \mod 2$ obviously only has the single solution $x \equiv 1 \mod 2$. When $n = 4$, there are exactly two solutions, $x \equiv 1, 3 \mod 4$. We claim that when $n = 2^e > 4$, there are exactly four solutions. First, notice that $x \equiv \pm 1, 2^{e-1} \pm 1 \mod 2^e$ are all solutions to $x^2 \equiv 1 \mod 2^e$. That $x \equiv \pm 1 \mod 2^e$ are solutions is obvious. For the other two, notice that $(2^{e-1} \pm 1)^2 = 2^{2e-2} \pm 2^e + 1$. As $e \geq 3$, we have $2e - 2 \geq e$, so $(2^{e-1} \pm 1)^2 \equiv 1 \mod 2^e$. Finally, notice that these four solutions are all distinct, since $e \geq 3$.

We now want to show that these four solutions are all the solutions to $x^2 \equiv 1 \mod 2^e$. Since $2^e \mid (x-1)(x+1)$, one of $(x-1), (x+1)$, and the other, is even. Since $(x+1) = (x-1)+2$, and both $(x-1), (x+1) \equiv 0 \mod 2$, we must have $(x-1), (x+1) \equiv 0, 2 \mod 4$. As a matter of fact, exactly one is equivalent to 0 mod 4, and the other is equivalent to 2 mod 4. For instance, suppose $2||(x+1)$. Then it must be the case that $2^{e-1}|(x-1)$, which implies that $x \equiv 1 \mod 2^{e-1}$, so that $x \equiv 1, 2^{e-1} + 1 \mod 2^e$. If $2||(x-1)$, we end up with the conclusion that $x \equiv -1, 2^{e-1} - 1 \mod 2^e$ instead. So the four solutions we listed are indeed all the solutions to $x^2 \equiv 1 \mod 2^e$, when $e \geq 3$.

We can now put this all together. Using the previous proposition, $x^2 \equiv 1 \mod n$ has $N_1 \ldots N_k$ solutions. If p_i is odd, then $N_i = 2$, while if $p_i = 2$, then $N_i = 1, 2, 4$, depending on whether $2||n, 4||n$, or $8|n$. One quickly checks that the product of these numbers is equal to the number in the statement of this proposition. □