M328K – Rusin – HW7 – ANSWERS

1. Show that if p is prime and a is not a multiple of p, then the integer $c = a^{p-2}$ is an inverse of a mod p. Use this to compute the inverse of 3 modulo 67. (Hint: $67 = 2^6 + 3$.)

ANSWER: Recall that c is the inverse of a iff $ac \equiv 1$ mod p. But indeed this is true by Fermat's Little Theorem.

The point of this exercise is that it gives us a way to compute inverses without (say) using the Euclidean algorithm (which was a method we used before). So for example the inverse of 3 modulo 67 would be 3^{65}. We can compute this easily by successive squaring: $3^2 \equiv 9$, $3^4 \equiv 81 \equiv 14$, $3^8 \equiv 196 \equiv -5$, $3^{16} \equiv 25$, $3^{32} \equiv 625 \equiv 22$, and $3^{64} \equiv 484 \equiv 15$; then $3^{65} \equiv 45$. Indeed this is the inverse of 3: $3 \cdot 45 = 1 + 2 \cdot 67$. In a similar way when $p - 2$ is less than 2^k, we can compute a^{-1} with k squarings and at most $k + 1$ multiplications mod p, which is pretty darn efficient!

2. Use the Chinese Remainder Theorem to show that if n is divisible by at least two different primes, then there exist integers x with $x^2 \equiv 1 \pmod{n}$ other than $x \equiv 1$ and $x \equiv -1$.

ANSWER: The premise is that that the factorization of n into prime powers involves at least two primes, so split the primes into two groups to write $n = ab$ where each of a and b are the products of the powers of some of the primes dividing n; in particular, they are coprime to each other.

Then the CRT asserts that there is an integer x which is congruent to $+1$ modulo a and congruent to -1 modulo b. It follows that x^2 is congruent to 1 modulo both of them and then (using the other half of CRT) must be congruent to 1 modulo $ab = n$.

It remains only to show that x is congruent to neither $+1$ nor -1 modulo n. Well, if x were congruent to -1 modulo n then it would be congruent to -1 modulo $a|n$; yet we chose x to be congruent to $+1$ modulo a, not -1. Similarly x cannot be congruent to $+1$ modulo n because it's not congruent to $+1$ modulo b.

Or is it? We chose x to be congruent to $+1$ modulo a, but it could *also* be congruent to -1 modulo a — this happens if and only if $a = 2$! So we have not accomplished our goal if $a = 2$ (or if $b = 2$). Well, we can still win if we choose a and b to be some other coprime factors of n. This is always possible except in two cases: when n is a power of just one prime, and when n is twice a power of just one odd prime. So as I announced in class you have to assume just a little bit more to complete this problem; assuming for example that n is a product of two different odd primes is enough.

3. Show that the system of congruences

$$x \equiv a \pmod{b} \qquad x \equiv c \pmod{d}$$

has solutions iff $a \equiv c \pmod{\gcd(b, d)}$. (You might want to make up some examples to test this, first.)

ANSWER: Let us write e for $\gcd(b, d)$ for brevity.

First of all, if there is such an integer x, then $x - a$ is a multiple of b and hence of e, too: $x \equiv a$ mod e. Likewise $x \equiv c$ mod e. By transivity $a \equiv c$ mod e.

To go in the other direction, let's assume $a \equiv c$ mod e. Since e is the *greatest* common divisor of b and d, by the Bezout theorem, e is a linear combination of b and d, and thus all multiples of e are as well. In particular we can write $a - c$ in the form $zd - yb$ for some integers z and y. But from $a - c = zd - yb$ we conclude $a + yb = c + zd$, which is then an integer x which is simultaneously congruent to a modulo b and congruent to c modulo d.

4. Find all integer solutions x to the congruence $3x^2 \equiv 23 \pmod{91}$.

ANSWER: First we can simplify the problem a bit by getting rid of the "3": multiply both sides by the inverse of 3 mod 91. Since $3 \cdot 30 \equiv -1$, it follows that the inverse of 3 will be $-30 = 61$. Thus x satisfies the original congruence iff $x^2 \equiv 23 \cdot 61 = 1403 \equiv 38$, Now, x will satisfy this congruence mod 91 iff it satisfies it both modulo 7 and modulo 13 (since 91=$7 \cdot 13$.) It's easy to solve the congruence modulo 13, since $38 \equiv 25 = 5^2$: both 5 and -5 are solutions and since 13 is prime, a quadratic can have at most two solutions modulo 13, so the complete solution set is the set of x which are congruent to either 5 or -5 modulo 13. But this information is actually irrelevant because there are NO solutions modulo 7: all squares are congruent to 1,2, or 4 mod 7, while $38 \equiv 3$. So our problem cannot even be solved modulo 7, let alone modulo 91!

5. Find all integer solutions x to the congruence $x^2 - 2x - 3 \equiv 0 \pmod{135}$.

ANSWER: In view of the Chinese Remainder Theorem, it will suffice to find all the integers x for which $x^2 - 2x - 3 = (x - 3)(x + 1)$ is simultaneously a multiple of 5 and a multiple of 27. Clearly both $x = 3$ and $x = -1$ are solutions, but we need to proceed a bit carefully to ensure that there are no others.

Obviously both $x = 3$ and $x = -1$ are solutions, and any integer x which is congruent to one of these modulo 5 will solve the congruence modulo 5. But as in the prrevious prolem we note that 5 is a prime and therefore there can be at most 2 solutions to a quadratic mod 5. Obviously that means we have found the complete solution set modulo 5.

In a similar way we see these are the only solutions modulo 3. Then we try lifting up the solutions to get solutions mod 9 (and eventually, mod 27). Any solution must be of one of two forms $x = 3 + 3k$ or $x = -1 + 3k$ for some integer k. Substituting into the polynomial $(x - 3)(x + 1)$ gives respectively $3k(4 + 3k)$ or $(-4 + 3k)(3k)$; in either case this is congruent to zero mod 9 iff k is a multiple of 3, say $k = 3L$. Thus the only integers that solve the congruence mod 9 are those of the form $x = 3 + 9L$ or $x = -1 + 9L$. Substituting again into the polynomial gives $9L(4 + 9L)$ resp. $(-4 + 3L)(9L)$, which is congruent to zero mod 27 iff L itself is a multiple of 3, from which we finally conclude that our integers x must be congruent to 3 or -1 modulo 27.

Combining the previous two paragraphs shows that the *only* integers which solve the original congruence mod 135 are those x which are congruent to -1 or 3 modulo 135.

EXTRA CREDIT! Sometimes we try to solve problems that involve multiple variables. For example we might be interested in finding *pairs* of integers (x, y) that satisfy one or more congruences. We might simply want to know whether any such pairs exist, or to know more generally how many pairs there are, or if possible we might want a list of all solutions (or a procedure that will generate them all). Here is an example: show that if p is an odd prime there there are exactly $(p-1)$ pairs (x,y) that satisfy $x^2-y^2 \equiv 1 \pmod{p}$. (We consider two pairs (x,y) and (x',y') to be the same iff $x \equiv x \pmod{p}$ and $y \equiv y' \pmod{p}$. So there are p^2 "points" on this strange "plane" and I am asking you to show that $p-1$ of them are on this "hyperbola".)

ANSWER: The trick is that $x^2 - y^2 = (x-y)(x+y)$!

If a is any nonzero congruence class modulo p, then a has an inverse b with $ab \equiv 1$. Let $x = (a+b)/2$ and $y = (a-b)/2$; then $x^2 - y^2 = ab \equiv 1$ so this pair (x,y) lies on the curve. (Note that $Z/2$ means $2^{-1}Z$, since 2 has an inverse modulo p because p is odd.) Conversely if $x^2 - y^2 = 1$ then let $a = x + y$ and $b = x - y$; these will be inverses of each other. Thus there are exactly as many points (x,y) on the curve as there are inverse pairs (a,b), and there are $p-1$ of those, one for each nonzero a modulo p.