M328K – Rusin – HW4 ANSWERS – Due TUESDAY, Feb 21 2017

1. Find all solutions to the following systems of equations:

(a) $x \equiv 3 \pmod{7}$ and $x \equiv 7 \pmod{3}$

(b) $x \equiv 5 \pmod{14}$ and $x \equiv 20 \pmod{21}$

(c) $x \equiv 5 \pmod{14}$ and $x \equiv 19 \pmod{21}$

ANSWER: (a) is standard Chinese Remainder: it's easy to spot that $x = 10$ is a solution, and then CRT assures us that the solution is unique modulo 21.

(b) has no solutions: if $x \equiv 5 \pmod{14}$ then it's also true that $x \equiv 5 \pmod{7}$; but if $x \equiv 20 \pmod{21}$ then we'd have $x \equiv 20 \pmod{7}$. Since $5 \not\equiv 20 \pmod{7}$, this is a contradiction. So no such x can exist.

(c) is more delicate. The first condition requires $x = 5 + 14k$ for some integer k; then the second requires $5 + 14k = 19 + 21n$ for some n, which in turn simplifies to $2k = 2 + 3n$. Thus n must be even, say $n = 2m$, in which case $k = 1 + 3n$, so that $x = 19 + 42k$. That is, the complete solution is $x \equiv 19 \pmod{42}$. Note that 42 is not the product of the moduli 14 and 21, but it is their lcm.

In the general case the analysis of a system of congruences can be done one prime at a time: if for any prime p there is a contradiction in the demands modulo (a power of) p, then there will be no solution; otherwise, use the CRT to find the unique solution modulo each prime power. The overall solution will be unique modulo the lcm of the moduli.

2. (a) Find an inverse of 10 modulo 121. (Hint: you might want first to find an integer y with $10y \equiv -1 \pmod{121}$.)

(b) Solve the congruence $10x + 23 \equiv 97 \pmod{121}$.

ANSWER: For (a) we observe $10 \cdot 12 \equiv -1$ so $10 \cdot -12 \equiv 1$, that is, the inverse of 10 is $-12 \equiv 109$. Then we can solve (b) by multiplying both sides of the congruence $10x \equiv 74$ by the inverse of 10. To do it by hand I might multiply by 12 instead to see $-x \equiv 12 \cdot 74 = 888 \equiv 41$, so $x \equiv -41 \equiv 80$.

3. There is a tool that people use to check their arithmetic, called "casting out nines". This is illustrated by the following example: if we need to compute $(12 \times 34) + 56$ we may do so longhand; I get $408 + 56 = 464$. In order to check this, we instead replace every integer encountered by the sum of its digits, replacing 12 by $1 + 2 = 3$, 34 by 7, and 56 first by 11 and then by $1 + 1 = 2$; this gives us a simpler computation to do: $(3 \times 7) + 2 = 21 + 2 \longrightarrow 3 + 2 = 5$ This is to be compared to the digit-sum for our proposed answer: $464 \longrightarrow 14 \longrightarrow 5$. The fact that we got the same single digit (namely 5) in both cases is a corroboration that we probably did not make any mistakes.

(a) Show by example that this technique can fail to catch some errors in addition.

(b) Explain why the technique does work, that is, if for every integer n we let $D(n)$ be the sum of the digits of n (written in base-10 notation) and let $E(n)$ be the result of applying D repeatedly until only a single digit remains, then show $E(n + m) = E(E(n) + E(m))$ and $E(n \times m) = E(E(n) \times E(m))$. (*Hint:* $10^k \equiv 1 \pmod{9}$ for every positive integer k. Now think about what "base-10 notation" means)

ANSWER: For (a) you could for example note that the calculation "$12+34=64$" passes the casting-out-nines test even though it's wrong. (Casting-out-nines can NEVER catch an erroneous interchange of digits.)

The reason CO9s works is because $E(n) \equiv n \pmod 9$ for every integer n. To see this, write n in its usual base-10 expansion:

$$n = \sum_{i=0}^{k} a_i 10^i$$

so the a_i are the digits of n. Then $D(n) = \sum_{i=0}^{k} a_i$, which is congruent to n itself modulo 9 because $10 \equiv 1 \pmod 9$ (and thus all powers of 10 are also congruent to 1). Then it follows that $D(D(n)) \equiv D(n) \equiv n$, $D(D(D(n))) \equiv D(D(n)) \equiv D(n) \equiv n$, etc. At some point the process stabilizes to $E(n) \equiv n \pmod 9$.

Now that we know $E(n) \equiv n$ for every integer n, we see that $E(n+m) \equiv n+m \equiv E(n)+E(m) \equiv E(E(n)+E(m))$; that is, if $A = n+m$ has been computed correctly, then $E(A)$ must agree with (the sum of the digits of) the sum of $E(n)$ and $E(m)$. Likewise for products: $E(n \times m) \equiv n \times m \equiv E(n) \times E(m) \equiv E(E(n) \times E(m))$; that is, if $A = n \times m$ has been computed correctly, then $E(A)$ must agree with (the sum of the digits of) the product of $E(n)$ and $E(m)$.

4. (a) Compute the 5th row of Pascal's Triangle.

(b) The ith term in the nth row of Pascal's Triangle equals

$$\frac{n!}{i!\,(n-i)!}.$$

Show that when n is prime, all entries of the nth row are multiples of n except the zeroth and the nth.

(c) Use the Binomial Theorem to show that when n is prime, $(1+1)^n \equiv 2 \pmod n$.

(d) Use induction to show that $k^n \equiv k$ for every $k = 1, 2, 3, \ldots$, again assuming n is prime.

ANSWER: The fifth row of Pascal's Triangle reads: 1, 5, 10, 10, 5, 1. Notice that all the terms except the ones on the ends are multiples of 5. That's not a fluke: the ith entry in the nth row is an integer $C(n,i)$ and, from the formula given, has the feature that $i!(n-i)!C(n,i) = n!$. The right side is obviously a multiple of n, so that n divides $i!(n-i)!C(n,i)$ too, and thus — assuming n is prime! — must divide one of those factors. It obviously cannot divide any of the factors in $i!$ or $(n-i)!$ because it's larger than them (unless $i = n$ or $i = 0$) so it must divide the last factor, $C(n,i)$.

By the Binomial Theorem, it then follows that if a and b are any integers, and n is prime, then $(a+b)^n = \sum_{i=0}^{n} C(n,i) a^i b^{n-i} \equiv a^n + b^n \pmod n$ since all the other terms in the sum are multiples of n. In particular, when $a = b = 1$ we have $(1+1)^n \equiv 1^n + 1^n$, that is, $2^n \equiv 2 \pmod 2$. Then proceed by induction: if you have already proved $k^n \equiv k$, it follows that $(k+1)^k \equiv k^n + 1^n \equiv k+1$ as well.

If k is not divisible by the prime n, you could then multiply both sides by the inverse of $k \pmod n$ and conclude that $k^{n-1} \equiv 1 \pmod n$, which is also good to know.

5. Is $2^{341} \equiv 2 \pmod{341}$? Is $3^{341} \equiv 3 \pmod{341}$? Is 341 prime?

ANSWER: Working modulo 341 I compute the first few powers of 2 to be

$$2^2 = 4, \quad 2^3 = 8, \quad \ldots, \quad 2^8 = 256, \quad 2^9 = 512 \equiv 171, \quad 2^{10} \equiv 341 \equiv 1$$

Then of course $2^{340} = (2^{10})^{34} \equiv 1$, too. So after working on problem 4 you might jump to the conclusion that 341 is prime, but of course it's not: $341 = 11 \cdot 31$.

If you had noticed that factorization in the first place, you could have proceeded differently: from problem 4 it follows that $2^{10} \equiv 1 \pmod{11}$ since 11 is prime. Also $2^5 = 32 \equiv 1 \pmod{31}$ so $2^{10} \equiv 1 \pmod{31}$ too. This shows that $2^{10} \equiv 1 \pmod{341}$, as already proved a different way.

You could similarly show that $3^{10} \equiv 1 \pmod{11}$ and $3^{30} \equiv 1 \pmod{31}$, so $3^{340} = 3^{11\cdot 30+10} \equiv 3^{10} \pmod{31}$, and I work out that last one to be 25 because $3^5 = 243 \equiv -5 \pmod{31}$. So 3^{340} cannot be congruent to 1 modulo 341 because it's not even congruent to 1 modulo 31. With an eye toward problem 4 again, this shows 341 is not prime.

You might find it amusing to note that $a^{560} \equiv 1$ for *every* integer a that's coprime to 561, and yet 561 is not prime. That is, 561 successfully manages not to reveal its compositeness no matter how many times we try to use the test from problem 4! Such numbers are called *pseudo-primes* and they are rarer than the primes themselves (even though there are infinitely many of them).

6-7. (a) Find all solutions to the congruence $x^2 \equiv 1 \pmod 8$

(b) Show that if p is prime and $x^2 \equiv 1 \pmod p$ then either $x \equiv 1 \pmod p$ or $x \equiv -1 \pmod p$. (Hint: Use Euclid's definition of "prime" on the premise that $p|(x^2-1)$.)

ANSWER: For (a) note that $(4k \pm 1)^2 = 16k^2 \pm 8k + 1 \equiv 1 \pmod 8$ for every integer k; it follows that *every* odd integer x solves the congruence $x^2 \equiv 1 \pmod 8$.

On the other hand, if p is prime and $x^2 \equiv 1 \pmod p$ then p divides $x^2 - 1 = (x-1)(x+1)$; from Euclid's characterization of primes that means p must divide either $x-1$ or $x+1$. In the first case $x \equiv 1 \pmod p$ and in the second case $x \equiv -1 \pmod p$.

8. Suppose $N = pq$ where p and q are both primes.

(a) Show that there exists an integer x with $x^2 \equiv 1 \pmod N$ but $x \not\equiv \pm 1 \pmod N$. (Hint: Chinese Remainder Theorem.)

(b) Show that if $y^2 \equiv 4 \pmod N$ and $y \not\equiv \pm 2 \pmod N$ then $\gcd(x-2, N)$ is one of the two prime divisors of N.

ANSWER: When p, q are distinct primes, then a congruence holds modulo pq iff it holds both modulo p and modulo q. As in problem 7 we see $x^2 \equiv 1 \pmod p$ is only possible if $x \equiv \pm 1 \pmod p$. An integer x which satisfies $x \equiv 1$ modulo both p and q will be congruent to 1 modulo N as well; likewise if $x \equiv -1$ modulo both p and q then $x \equiv -1 \pmod N$. No interesting solutions x so far. BUT: we also get a solution to our original congruence if

$x \equiv 1 \pmod{p}$ while $x \equiv -1 \pmod{p}$ or vice versa, and the Chinese Remainder Theorem assures us that there are such x.

You might try working out an example: $x^2 \equiv 1 \pmod{15}$ iff $x \equiv 1, -1, 4, or - 4$, and 4 is the unique congruence class modulo 15 which is congruent to $+1$ modulo 3 and congruent to -1 modulo 5.

I also added this challenge: "If you have a computer package that can handle large integers, you might try for example to factor $N = 1545013$ using the fact that $53405^2 \equiv 27$ and $177573^2 \equiv 12 \pmod{N}$ ".

The idea for this one is to observe that from the data given we conclude $2^2 \cdot 53405^2 \equiv 108 \equiv 3^2 \cdot 177573^2 \pmod{N}$, i.e. N divides $(2 \cdot 53405)^2 - (3 \cdot 177573)^2 = (2 \cdot 53405 - 3 \cdot 177573) \cdot (2 \cdot 53405 + 3 \cdot 177573)$ and thus every prime divisor of N divides this product too, and so must divide one of the factors — but some primes might divide the first factor 425909 and some divide the second factor 639529. Indeed we can then use the Euclidean Algorithm to quickly compute the gcds of these integers with N; they are 1249 and 1237 respectively, and indeed we have just found the prime divisors of N!

9. Recall that our *definition* of the Euler ϕ-function is that $\phi(n)$ is the number of integers in $\{0, 1, \ldots, n-1\}$ which are coprime to n. Use this definition to show that $\phi(n)$ is even for every integer $n > 2$.

ANSWER: For each a coprime to n we find $\gcd(n-a, n) = \gcd(a, n) = 1$ so that $n - a$ is also among the coprime integers. That is, the integers we are counting come in pairs, a and $n - a$ (one less than $n/2$ and one greater than $n/2$). When you're counting objects that come in pairs there's obviously an even number of them!

There is an exception: $\phi(2) = 1$ is odd. How did that happen? It's because for $n = 2$ and $a = 1$ we have $n - a = a$ again: there's not really a *pair* here. But in order for this to happen we need $n = 2a$, in which case $\gcd(n, a) = \gcd(2a, a) = a$; unless $a = 1$ (so that $n = 2$), this means a will not be coprime to n.

10. Show that if $m|n$ then $\phi(m)|\phi(n)$.

ANSWER: There are more interesting proofs I can use here but let's simply use the formula I gave in class:

$$\phi(n) = n \cdot \prod_{p|n} (1 - \frac{1}{p})$$

So if $m|n$, say, $n = mk$ for some integer k, then all the primes dividing m will also divide n, giving a lot of cancellation in

$$\frac{\phi(n)}{\phi(m)} = \left(\frac{n}{m}\right) \prod (1 - \frac{1}{p}),$$

where the only factors left in the product are those for primes p which divide n but not m. But in this case they divide k; write $k = k' \cdot k''$ where k'' is the product of all these primes. In that case the right-hand side above will be just $k' \cdot \prod (p-1)$ which is an integer. Thus $\phi(m)$ divides $\phi(n)$.