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

My apologies for being late to distribute this HW. How about if I move the due date back one class? That way you will be turning this in just before the first midterm.

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 $x \equiv 19 \pmod{21}$

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 $10x + 23 \equiv 97 \pmod{121}$.

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)

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.

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

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

7. (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 $p|(x^2-1)$.)

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.

Remark: This last observation is really important. Since computing gcd's (by the Euclidean Algorithm) is really very easy (for a computer), a small generalization of this last exercise says more generally that you can find a factor of a big number N almost instantly if you can find a number (other than the obvious one) whose square is a small perfect square mod N. It turns out that there are ways to do this, faster than you might expect. This led to factorization programs which were considered very good in the early computer days.

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 $177573^2 \equiv 12 \pmod{N}$

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 $n > 2$.

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