M328K – Rusin – HW7 – Due Tuesday, Apr 11 2017

Here are a few solved problems you can use as warm-up: try sect. 4.2#9, sect. 4.3#13, sect. 4.4#1

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: $67 = 2^6 + 3$.)

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 $x \equiv -1$.

Remark: one way to factor integers is to look for such integers x (there are some clever ways to do so) and then use the Euclidean algorithm to compute $\gcd(x-1, n)$.

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.)

Sometimes you should use multiple tools on one problem:

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

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

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".)