Number Theory, hw4

Ethan D. Bolker

October 2, 2013

Note: If the Brown freshmen for whom Silverman wrote this book can do the problems then UMass math majors surely can. Prove me right.

1. Silverman, Exercise 10.1.

2. Silverman, Exercise 10.2.

3. Silverman, Exercise 10.3.

4. Read and understand the proof of the Chinese Remainder Theorem at `http://crypto.stanford.edu/pbc/notes/numbertheory/crt.xhtml`. (It uses the knowledge we have about which numbers have multiplicative inverses in $\mathbb{Z}_n$. I like it better than the one in Silverman.)

   Use the algorithm from that proof to answer Silverman 11.5.

   Doing it by hand will be good practice using the Euclidean algorithm to find multiplicative inverses but you might be better off working with an online number theory calculator. You might want to explore `http://www.math.uconn.edu/~kconrad/math3240f09/calc.html`. Look around for other tools (online calculators or downloadable applications). Let me know if you find anything useful.

5. Consider the following statements about an odd prime p:

   - $p \equiv 1 \mod 4$.
   - p is a sum of two integer squares.
   - -1 has a square root in $\mathbb{Z}_p$.

These are in fact equivalent. Any one of them implies the other two. Proving that was one of Fermat's major accomplishments. Here's your assignment now:

(a) Verify the equivalence for all the odd primes less than 100.

(b) Prove as many of the six possible implications as you can. (Some are really easy. Some are really hard.)

6. Approximating $\sqrt{2}$.

The Diophantine equation

$$x^2 - 2y^2 = 0.$$

has no solutions. If it did, then x/y would be a rational number whose square was 2. That's impossible.

But we can get close. For example,

$$7^2 - 2 \times 5^2 = -1$$

so

$$\left(\frac{7}{5}\right)^2 = 2 - \frac{1}{5^2} \quad .$$

Your job: find enough solutions to the Diophantine equation

$$x^2 - 2y^2 == \pm 1$$

to guess (and prove) a pattern that produces infinitely many solutions. Then find one big enough to produce a rational number whose square is between 1.999999999 and 2.000000001.

Hint to get you started. There are several solutions *smaller than* (7,5).