Number Theory, hw3

Ethan D. Bolker

October 7, 2013

1. Silverman, Exercise 9.1.

2. Silverman, Exercise 9.2.

   Hint for part (b). When (if ever) is an element $a \in \mathbb{Z}_p$ its own multiplicative inverse? When it's not, what is going on?

3. Quadratic equations

   Let p be a prime. We know that the linear congruence

   $$ax + b \equiv 0 \mod p$$

   has a unique solution when $a \not\equiv 0$. Now let's think about the *quadratic* equation

   $$ax^2 + bx + c \equiv 0 \mod p \tag{1}$$

   for *odd* primes p.

   (a) Show that the usual quadratic formula finds the roots of Equation 1 when the discriminant $\Delta = b^2 - 4ac$ has a square root in $\mathbb{Z}_p$.

   Note: You don't have to *derive* the quadratic formula. You just have to show that it produces the roots.

   (b) Show that each element of $\mathbb{Z}_p^*$ has either two square roots or none.[1]

   Solution: Here's the idea. If an element of $\mathbb{Z}_p$ has one square root then finding a second one is easy, since $(-x)^2 = x^2$. I just need to make sure those are different. Then I need to make sure there are no others. That's not true when the modulus is 8, so to prove it here I know I'll have to use the the fact that p is prime.

   Suppose $a \in \mathbb{Z}_p^*$ has a square root x. Then $x^2 \equiv (-x)^2 \equiv a \mod p$ so $-x$ is also a square root of a. Since $x \not\equiv -x \mod p$ I have two square roots.

   Let y be a square root of $a \mod p$. I need to show that $y \equiv \pm x \mod p$. That's easy:

   $$x^2 \equiv y^2 \mod p$$

   implies

   $$p | y^2 - x^2 = (y - x)(y + x).$$

   I know that when a prime divides a product it divides one of the factors, so p divides $y - x$ or $y + x$. That means $y \equiv -x \mod p$ or $y \equiv x \mod p$.

[1] $\mathbb{Z}_p^*$ is the set of *nonzero* elements of $\mathbb{Z}_p$.

4. Use Fermat's Little Theorem to show that

$$a^{(p-1)/2} \equiv \pm 1 \mod p.$$

Solution: This is easy. Fermat's Little Theorem tells me that

$$(a^{(p-1)/2})^2 = a^{p-1} \equiv 1 \mod p.$$

Since I just finished proving that 1 has only two square roots, ± 1, $a^{(p-1)/2}$ must be one of them.

Several of you got the logic backwards here. Please read carefully.

5. Who has a square root?

Investigate the set S_p of elements of $\mathbb{Z}_p^*$ that have square roots.

It's very hard to detect a pattern that tells you when a particular element has a square root. Finding that pattern is one of the goals of this course. But there are several parts of the pattern that we can begin to see now.

(a) Start with some calculations: Find S_p for $p = 5, 7, 11, 13$ and maybe some larger values – perhaps 29 and 31. Consider doing this collaboratively – parcel out some larger primes among the class and pool your results. As you do the work you should stumble on arithmetic shortcuts that will in fact help you understand what's happening.

(b) How many elements are there in S_p? (Make a conjecture. Prove it if you can.)

(c) A previous problem in this homework leads to a conjecture relating S_p to the computation $a^{(p-1)/2}$. Find that conjecture and prove it if you can.

(d) Clearly $1 \in S_p$ since ± 1 are its square roots.[2] Can you guess/conjecture of the form

$$-1 \text{ has a square root} \mod p \text{ if and only if } p \ldots$$

6. More proofs of Fermat's Little Theorem. The Wikipedia article at `http://en.wikipedia.org/wiki/Proofs_of_Fermat's_little_theorem` offers several proofs of Fermat's Little Theorem. I recommend two of these: **Proof by counting necklaces** and **Proof using the binomial theorem**. Read and understand them. To convince yourself and me that you do really understand, find the step in each proof where you use the hypothesis *p is prime* and find an example to show how that step fails when the hypothesis is false.

[2] Remember that in $\mathbb{Z}_p$, -1 is $p - 1$.