Math 2020 — Spring 2011

Solving Discrete Problems — P. Achar

Homework Set 9b

Due: April 15, 2011

I will add points for Problems 1 and 2 to your score for Homework 9. For Problem 3, you should make a serious attempt to formulate a conjecture based on the examples you work out, but the points will be for "effort."

1. Let p be a prime number. Prove that if $a^2 \equiv b^2 \pmod p$, then either $a \equiv b \pmod p$ or $a \equiv -b \pmod p$. (*Note:* This fact is something you've probably "taken for granted" in $\mathbb{Z}$ or $\mathbb{R}$, but it requires proof even in those settings. If n is *not* prime, the corresponding statement in $\mathbb{Z}_n$ is false. For instance, see if you can find an element of $\mathbb{Z}_9$ with more than two square roots.)

2. How many elements of $\mathbb{Z}_p$ have a square root? You must prove your answer, of course. This means: you must make a list of elements that have square roots, and prove that your list doesn't contain repeats and doesn't omit any elements that do have a square root. (*Hint:* $\mathbb{Z}_p$ has p elements in all. If you square all of them, you'll get a list of all the elements that have square roots, but you'll definitely have repeats in the list. How many elements must you remove to eliminate repeats? This is related to the previous question.)

3. The number -1 doesn't have a square root in $\mathbb{Z}$ or $\mathbb{R}$, but sometimes, it has a square root in $\mathbb{Z}_p$.

   Check the first few odd prime numbers ($p = 3, 5, 7, 11, 13, \dots$) to see whether the equation $x^2 \equiv -1 \pmod p$ has a solution. Make a conjecture about the conditions on p under which this equation has a solution. Your conjecture should have the following form

   > Assume p is an odd prime number. The equation $x^2 \equiv -1 \pmod p$ has a solution if and only if $\dots$ (*some statement about* p).

   Challenge Problem: Prove your conjecture. (This is much harder than the usual "Bonus" problems. There are easyish proofs using ideas from group theory beyond what we will cover this semester, but I don't know if there is a proof using only what we've learned about modular arithmetic so far. If you find one, that'll be very impressive!)