

Math 152, Spring 2006, Problem Set 2 (Part I of II)  
Due: Friday, April 21

If you have Cox's book, then the description is easy: problems 1.1, 1.3, and 1.4. I've written these out below (with extra commentary) in case you don't have the book yet.

On Monday, I'll assign some very straightforward additional exercises dealing with quadratic congruences.

1. (1.1 in Cox) In the proof on primes of the form  $p = x^2 + y^2$ , we used a lemma whose starting point was the following identity:

$$(x^2 + y^2)(z^2 + w^2) = (xz \pm yw)^2 + (xw \mp yz)^2$$

This was very desirable because it says, in particular, that the property of being the sum of two squares is actually preserved under multiplication. If we wanted to prove a DESCENT step for primes of the form  $p = x^2 + ny^2$ , we might hope that the analogous property is preserved. Somewhat miraculously, it is.

- (a) Prove the following identity

$$(x^2 + ny^2)(z^2 + nw^2) = (xz \pm nyw)^2 + n(xw \mp yz)^2$$

i.e. that being a number of the form  $x^2 + ny^2$  is preserved under multiplication. (Note: this generalizes the earlier identity, which we recover by setting  $n = 1$ .)

- (b) Generalize part (a) even further. Find expressions  $\clubsuit$  and  $\spadesuit$  which make the following identity true:

$$(ax^2 + cy^2)(az^2 + cw^2) = (\clubsuit)^2 + ac(\spadesuit)^2$$

2. Let  $n$  be a positive integer.

- (a) Prove the following generalization of the LEMMA we used in class:

If  $N = a^2 + nb^2$  with  $a, b$  relatively prime, and  $q = x^2 + ny^2$  is a prime divisor of  $N$ , then  $N/q = z^2 + nw^2$  for some integer  $z, w$  with  $\gcd(z, w) = 1$ .

- (b) Show that your proof in (a) still works if  $q = 4$  and  $n = 3$  (that is, even though  $q$  isn't a prime in this case).

3. Prove the DESCENT step for primes of the form  $x^2 + 2y^2$  and  $x^2 + 3y^2$ . You should mimic the proof of the DESCENT step we did in class. For  $n = 2$ , use the previous exercise as a starting point to show:

If  $p|a^2 + 2b^2$  for some  $a, b$ , with  $\gcd(a, b) = 1$ , then  $p = x^2 + 2y^2$  for some  $x, y$ .

For  $n = 3$ , prove the statement that if  $p$  is an ODD prime and  $p|a^2 + 3b^2$  with  $\gcd(a, b) = 1$ , then  $p = x^2 + 3y^2$  for some  $x, y$ . (This question is a little harder than  $n = 2$  since the descent argument fails for  $q = 2$  (WHY?) so you need to produce a sequence of ODD primes  $q < p$  if  $p \neq x^2 + 3y^2$  for any  $x, y$  to derive a contradiction. Using (b) of the previous exercise should help.)