

## BASIC NUMBER THEORY, PROBLEM SET 2

### Primes and Unique Factorization

- (1) (a) Create a list of all of the primes less than 200, using the following method (which is known as the *Sieve of Erathosthenes*). Write out a list of the numbers from 1 to 200, and cross out 1. The smallest number left which isn't crossed out is 2, which is prime, so circle 2 and cross out every larger multiple of 2. Repeat the process, always circling the smallest number that isn't crossed out and then crossing out its multiples. Explain why the prime numbers less than 200 are exactly the circled numbers.  
(b) In the above exercise, why didn't you cross out any new numbers after you circled 17?
- (2) Prove that any prime of the form  $3k + 1$  is also of the form  $6k + 1$ .
- (3) What does it mean for two integers to be relatively prime, in terms of the exponents of the primes in their unique factorizations?
- (4) A number  $N$  is said to be *square-free* if 1 is the only square number which divides  $N$ .
  - (a) What does it mean to say that  $N$  is square-free, in terms of the exponents of the primes in the unique factorization of  $N$ ?
  - (b) What is the largest number of consecutive square-free positive integers?
  - (c) Provide a definition and repeat the previous parts for  $n^{\text{th}}$ -power-free integers.
  - (d) For any positive integer  $k$ , find  $k$  consecutive composite numbers.
- (5) Determine whether the following assertions are true or false. If true, prove the result, and if false, give a counterexample.
  - (a) If  $a^3|c^3$ , then  $a|c$ .
  - (b) If  $a^3|c^2$ , then  $a|c$ .
  - (c) If  $a^2|c^3$ , then  $a|c$ .
  - (d)  $[a^2, ab, b^2] = [a^2, b^2]$ . (Recall that  $[x, y]$  is the LCM of  $x$  and  $y$ .)
- (6) If  $2^n + 1$  is an odd prime for some integer  $n$ , show that  $n$  is a power of 2.
- (7) If  $2^n - 1$  is a prime for some integer  $n$ , show that  $n$  is itself a prime.
- (8) Show that 24 is the largest integer divisible by all integers less than its square root.

### Miscellaneous and Harder Problems

- (9) (a) Show that every positive integer  $n$  can be written uniquely in the form  $n = ab$ , where  $a$  is square-free and  $b$  is a square.  
(b) Suppose that there are  $t$  positive primes smaller than  $n$ . Using the previous part of this problem, prove that  $2^t \sqrt{n} \geq n$ , and conclude that  $t > \frac{1}{2} \log_2 n$ .
- (10) (a) Mimicking Euclid's proof of the infinitude of primes, give a proof that there are infinitely many primes of the form  $4k + 3$ .  
(b) Find a similar proof that there are infinitely many primes of the form  $4k + 1$ . (Be careful, this will take more thought than the  $4k + 3$  case.)
- (11) Suppose we have a more general setting in which divisibility is defined. (I'm being quite purposely vague here. I'll give examples of what I mean by a "more general setting" in a moment.) Define *units* to be numbers which divide 1 (so the units of  $\mathbb{Z}$  are  $\pm 1$ ). Next, we define *primes* to be numbers  $p$  which aren't units and which possess the property that  $p|ab$  implies either  $p|a$  or  $p|b$ , and we define *irreducibles* to be numbers  $\mathfrak{p}$  which aren't units and such that  $\mathfrak{p} = ab$  implies that one of  $a, b$  is a unit.
  - (a) If  $p$  is a prime, show that  $p$  is also an irreducible.

- (b) For integers, we proved in class that irreducibles are also primes. However, this proof required the Division Algorithm in a key step, and so unless we have an analogue of the Division Algorithm in our more general setting, the set of primes and the set of irreducibles may not coincide. Since the proof of unique factorization of the integers used the fact that irreducibles and primes are the same thing, we may not get unique factorization in our more general setting! As an example, let  $S$  be the set of numbers of the form  $a + b\sqrt{-5}$ . Observing that  $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ , show that  $\pm 1$  are the only units of  $S$  and that  $2, 3, 1 + \sqrt{-5}$ , and  $1 - \sqrt{-5}$  are all irreducibles. Conclude that 6 doesn't factor uniquely into irreducibles. (Hint: consider the complex absolute value  $N(a + b\sqrt{-5}) = a^2 + 5b^2$ . Show that  $N$  is multiplicative, i.e.  $N(\alpha\beta) = N(\alpha)N(\beta)$  for  $\alpha, \beta$  in  $S$ . By considering the possible values for  $N$ , show that  $2, 3, 1 + \sqrt{-5}$ , and  $1 - \sqrt{-5}$  are all irreducibles.)
- (c) Next, consider the set  $T$  of numbers of the form  $a + bi$ , where  $a$  and  $b$  are normal integers and  $i$  is the square root of  $-1$ . (We call  $T$  the "Gaussian integers".) We will show that there is a Division Algorithm for  $T$ . To begin with, let  $N(a + bi) = a^2 + b^2$ , and show that  $N$  is multiplicative. To make our Division Algorithm, we want to show that for  $a, b$  in  $T$ , there are  $q$  and  $r$  in  $T$  such that  $b = qa + r$  and  $N(r) < N(a)$ . Select  $q$  by finding the Gaussian integer closest to  $b/a$ , and show that this selection works.
- (d) Using the previous part, conclude that primes and irreducibles are the same in the Gaussian integers, and that we therefore obtain unique factorization in the Gaussian integers. Experimentally investigate which integer primes are still primes in the Gaussian integers. For example, 3 is still prime, whereas  $2 = (1 + i)(1 - i)$  and  $13 = (3 + 2i)(3 - 2i)$ . Any conjectures?