Exercises E5: Number Theory

August 31, 2006

1 From *Making, Breaking Codes* by Paul Garrett

Original problem numbers in parens. Note Optional, DOUBLE and TRIPLE point scores. Garrett has appendix of problem answers.

1. Prove directly from the definition of divisibility that if $d \mid m$, then $d \mid (-m)$. (7.1.07)

2. Observe that 1331 and 14641 cannot be prime, without computation. (7.1.08)

3. Find the smallest divisor $d > 1$ of 12344321. (7.1.11)

4. (Optional) Show that for any integer n, the two integers n and $n+1$ are always relatively prime. (7.1.14)

5. (Optional) TRIPLE POINTS. How likely is it that two randomly chosen positive integers will be relatively prime? (7.1.20)

6. (Optional) Find a proper factor of 101,010,101,010,101 without using a calculator. (7.2.04)

7. Explain why $2^m + 1$ cannot possibly be a prime number unles m is a power of 2. (7.2.08)

8. DOUBLE POINTS. (*This is Euclid's proof of the infinitude of primes.*) Suppose there are only finitely many primes $p_1, p_2, \cdots, p_n$. Consider the number $N = p_1 p_2 \cdots p_n + 1$. Show that none of the p_i can possibly divide N. Conclude that there must be some other prime than those on the list: contradiction. (7.2.12)

9. For an integer n, show that the greatest common divisor of the two integers $n^3 + n^2 + n + 1$ and $n^2 + n + 1$ is invariably just 1. (7.3.08)

10. (Optional) Find a multiplicative inverse to $n \bmod n^2 + 1$. (7.4.09)

11. As usual, denote the integers $\bmod n$ by $\mathbf{Z}/n$. How many members does $\mathbf{Z}/n$ have? (7.7.03)

12. (Optional) As usual, denote the integers $\bmod n$ that are relatively prime to m and thus have multiplicative inverses by $\mathbf{Z}/m^\times$. How many members does $\mathbf{Z}/m^\times$ have? (7.7.04)

13. (Optional) Compute $2^{1000}\%11$ (Don't use numbers much larger than 11). (7.7.09)

14. Show that $x^3 + y^3 = 3$ has no solution in integers (Hint: look at this mod 7: that is, see what the cubes are mod 7.) (7.7.17)

15. (Optional) The Cocoanut problem: Three sailors are shipwrecked on an island where they find a monkey and a lot of cocoanut trees. They pick N nuts for a food supply and put them in a pile.

During the night, the most distrustful sailor sneaks up and takes his fair share by dividing the pile into three and hiding his one-third share. There is a nut left over, which he gives to the monkey before going back to sleep. Each of the other sailors does the same thing: divides the remaining pile into three, taking and hiding his third, and giving the lone remaining nut to the monkey. In the morning the 3 sailors meet, divide the remaining pile into three, each taking his third. Surprisingly, there is a nut left which, believe it or not, is given to the monkey. What is the minimum number of cocoanuts that could have been in the original pile?

16. Casting out nines: a cute method of checking your arithmetic. Show that for an integer $n = a_k \cdots a_2 a_1 a_0$ with decimal digits $a_k, \cdots, a_2, a_1, a_0$, that $n \equiv a_k + \cdots + a_2 + a_1 + a_0 \bmod 9$.

Now explain how to check the addition and multiplication of large integers by casting out nines. (7.7.20)

17. Find the ('discrete') logarithm of 3 base 2 mod 125. (7.8.11)

18. (Optional) Prove that for any two different primitive roots r and s modulo m, and letting $\log_r$ and $\log_s$ denote discrete logarithms base r and base s modulo m, respectively, we have the identity

$$\log_r x = \log_r s \cdot \log_s x$$

for any x that is nonzero modulo m. (7.8.13)

2 From Trappe and Washington

Section 3.13

For now, consider only exercises 1 — 28.

Exercises: 1, 2, 3, 4, 5, 7, 9, 10, 12, 14, 15, 17, 19, 22, 24, 25, 27.

All Trappe exercises (from 1 — 28) not listed above are optional.