

MA357, Spring 2008 — Problem Set 4

This is a short assignment intended to keep you busy this week. Congruences galore, the ϕ function, and the Chinese Remainder Theorem. Plus, of course, some random other stuff. A write-up of all the problems except the ones labelled “to explore” is due on **Friday, March 21**.

1. Show that for any positive integer n , the number $1^n + 2^n + 3^n + 4^n$ is divisible by 5 if and only if n is not divisible by 4. (“Hey, Little Fermat!”)

2. Show that if n is an integer, then so is

$$\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}.$$

(Remember that mod 15 is the same as mod 5 and mod 3 simultaneously.)

3. Show that if $n \geq 2$ is not a prime number, then $2^n - 1$ is not a prime number. (Remember how to factor $x^k - 1$...) Show by examples that if n is a prime, $2^n - 1$ may or may not be a prime. (Primes of this form are called *Mersenne primes*.)

4. Silverman, Exercise 9.2.

5. Suppose p and q are primes, and q divides $2^p - 1$. Prove that there exists a k such that $q = 2kp + 1$. (Hint: what is the order of 2 modulo q ?)

Explain how one might use this result to show (without using a computer) that $2^{17} - 1$ is prime.

6. Do any numbers satisfy the equation $\phi(n) = 2n$?

7. Do any numbers satisfy the equation $\phi(n) = n/2$?

8. A band of 17 pirates, upon dividing their gold coins, found that three coins remained after the coins had been apportioned evenly. In the ensuing brawl, one of the pirates was killed. The wealth was again redistributed equally, and this time ten coins remained. Again an argument broke out and one of the pirates was killed. This time the fortune was distributed evenly among the survivors. What is the least possible value for the number of coins the pirates had initially?

To Explore: We sorted out in class how to solve linear diophantine equations such as $ax + by = c$. But we didn't come close to exhausting the subject. This exploration considers various related questions:

- a. Suppose a and b are positive. For which positive integers c do there exist *positive* integers such that $ax + by = c$?

- b. Work out how to solve linear diophantine equations with more variables, such as $ax + by + cz = d$.
- c. What if we put both extensions together, and ask for solutions (or conditions for solvability) for the general equation

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

with the conditions that all the x_i should be positive?

(See also problems 6.4 and 6.6 in Silverman.)

To Explore: “Round numbers” are numbers that are highly divisible by 10 (or sometimes by 5). Let’s generalize that to say that “round numbers” have lots of divisors. This sort of justifies the following definition:

Definition: A number n is called *very round* if it has the property that any $a < n$ which is relatively prime to n is either prime or equal to 1. In symbols, for any $a < n$ we have

$$\gcd(a, n) = 1 \implies a = 1 \text{ or } a \text{ is prime.}$$

This captures the concept we want because it basically says that it is very hard for any number to fail to have a factor in common with n .

- a. Compile a complete list of very round numbers.
- b. Prove that your list is complete.
- c. Since there are very few very round numbers, it’s not such a good concept after all. Can you improve on it?
- d. People who work on factoring sometimes talk about “smooth” numbers. Find out what they are. How do they relate to this discussion?

To Explore: If we take “Fermat’s Little Theorem” and multiply through by a , we see that if p is a prime then $a^p \equiv a \pmod{p}$. (Little Fermat requires $a \not\equiv 0$, but this version works even if $a \equiv 0$.) This is actually how Fermat first stated the theorem. If we remembered it wrong, however, we might say something like $a^{n+1} \equiv a \pmod{n}$. This is hardly ever going to be true! Still, there are some numbers n such that this congruence holds for every integer a . Find them.