189-346/377B: Number Theory
Assignment 1

Due: Monday, January 29

1. Compute the greatest common divisor of 4655 and 12075 and express the result as a linear combination with coefficients in $\mathbf{Z}$ of these two integers.

2. Compute the multiplicative inverse of 2 in $\mathbf{Z}/65537\mathbf{Z}$.

3. If a and b are two relatively prime integers, and p is an odd prime, show that $a+b$ divides a^p+b^p, and that $\gcd(a+b,(a^p+b^p)/(a+b))$ is equal either to 1 or p.

Suppose that (a,b,c) is a solution to Fermat's equation $a^p+b^p=c^p$, and that p does not divide c. What can you conclude about $a+b$?

4. The Euclidean algorithm for computing the gcd of a and b, with $a>b$, relies on the fact that $\gcd(a,b)=\gcd(a_n,b_n)$, where the sequences a_n and b_n are defined recursively by the conditions $(a_0,b_0)=(a,b)$ and

$$b_{n+1} = \text{ remainder in the division of } a_n \text{ by } b_n; \quad a_{n+1}=b_n.$$

Show that $b_{n+2} \le b_n/2$, and conclude that the Euclidean algorithm terminates before the N-th step, where $N = 2\log(|b|)/\log(2)$. (Recall the convention that log is the natural logarithm–to the base e–although this does not matter here.)

5. Let $f \in \mathbf{Z}[x]$ be a polynomial with coefficients in $\mathbf{Z}$. Fix an integer N and denote by $[a]$ the remainder after deivision of a by N. Show that the sequence $[f(0)],[f(1)],[f(2)],\ldots,$ is periodic and that its smallest period divides N. What about the exponential sequence $[a^1],[a^2],[a^3],\ldots$?

6. Show that if $N=2^p-1$, with p a prime, then N divides 2^N-2.

7. Let $N = 2^{2^5} + 1$. Find an integer a such that $a^2 \equiv 1 \pmod{N}$ but such that $a \not\equiv \pm 1 \pmod{N}$.

8. What is $\phi(1) + \phi(2) + \cdots + \phi(n)$? How many fractions a/b are there in lowest terms satisfying $1 \leq a < b \leq n$?

9. Show that the set $\mathbf{Z}_5$ of 5-adic numbers contains an element i satisfying $i^2 = -1$, $5|(2-i)$. Compute i to 5 significant digits (i.e., modulo 5^5.)

10. According to the RSA cryptography scheme, a message M—described as a string of digits, with the convention that "a" corresponda to "01", "b" to "02", ... "z" to "6", and a blank space to "00" - is replaced by its coded version $C = M^e \pmod{n}$, where e and n are publicly available, but the factorization of n is kept secret. Consider the coded message

$$C = 1457235305057083460588973150001511738645389195888990$$

encoded with the RSA public key

$$n = 17025863870545887144908490224619062098783164408077639, \quad e = 5.$$

Knowing that the prime factorization of n is pq, where

$$p = 14732265321145317331353282383, \quad q = 1155685395246619182673033,$$

find the secret message M. (Caveat: In the course of your calculation, you will need to compute x^y mod z, where x, y and z are large. This calculation, done properly, should take a fraction of a second on a PC. If your calculation takes longer than this, beware that your machine is not first computing the number x^y, and only then reducing mod z (once it gets to that stage, which of course it never will...).

The next questions are intended only for students in Math 377.

11. Returning to question 4, show that the constant $2/\log(2) = 2.88...$ that appears in the running time analysis of the Euclidean algorithm can be improved to $1/\log(\frac{1+\sqrt{5}}{2}) = 2.07808....$

12. Describe an improvement of the Euclidean algorithm which is guaranteed to terminate in at most $\log(n)/\log(2) = 1.4427...\log(n)$ steps.

13. Let n be an integer. Show that the decimal (base 10) expansion of $1/n$ is ultimately periodic, and that the length of the smallest period divides the value $\phi(n)$ of the Euler ϕ-function at n. What if base 10 is replaced by some other base?