189-346/377B: Number Theory

Correction to assignment 2

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.

A direct application of the algorithm for gcd seen in class.

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

Using the gcd algorithm, and the fact that $\gcd(2, 65537) = 1$, we can write 1 as a linear combination of 2 and 65537:

$$1 = a \cdot 2 + b \cdot 65537.$$

Then a (or rather, its residue class mod 65537) is the sought-for inverse. Of course, in this case there is an easy short-cut: you can just take $a = (65537 + 1)/2$...

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.

If you carry out the polynomial division, viewing $a + b$ and $a^p + b^p$ as polynomials in a and b, you will see that

$$a^p + b^p = (a + b)(a^{p-1} - a^{p-2}b + a^{p-3}b^2 - \cdots + b^{p-1}).$$

Now, if you attempt to divide the second factor $h(a, b)$, in the factorisation above by $(a + b)$, viewing these objects again as polynomials in a and b, by constantly eliminating the terms involving powers of a, you are left with a remainder of pb^{p-1}. So if a prime ℓ divides $(a + b)$ and $h(a, b)$, it must also divide pb^{p-1}. But the prime ℓ cannot divide b, for otherwise it would also

have to divide a, since it divides $a+b$, but this is impossible since a and b are assumed relatively prime. So any common divisor of $a+b$ and $h(a,b)$ must necessarily divide 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 $a+b$?
If p does not divide c, then it does not divide $(a+b)$, and therefore the gcd of $(a+b)$ and $h(a,b)$ must be 1. But since the product $(a+b)h(a,b)$ is a perfect pth power, it then follows from unique factorisation in $\mathbf{Z}$ that $(a+b)$ (viewed now as an integer, not a polynomial!!) is itself a perfect p-th power, i.e., $a+b=d^p$ for some integer d. This type of observation was the starting point for the most ambitious attacks on Fermat's Last Theorem that were launched in the 19th century and throughout the first half of the 20th century.

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 $b_{n+2} \leq b_n/2$, 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.)

The key observation is that, given (a_{n+1}, b_{n+1}) with $a_{n+1} \geq b_{n+1}$, the remainder b_{n+2} is smaller than $a_{n+1}/2$. If $b_{n+1} \leq a_{n+1}/2$, this follows from the fact that $b_{n+2} < b_{n+1}$. If $b_{n+1} > a_{n+1}/2$, then the remainder in the division of a_{n+1} by b_{n+1} is just $a_{n+1} - b_{n+1}$, which is less than $a_{n+1}/2$. The result now follows from the fact that $a_{n+1} = b_n$.

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 division 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 $[a^1], [a^2], [a^3], \ldots$?

The first statement is a direct property of congruences. As for the second,

the key point to observe was that, if a is relatively prime to N, then the period in the sequence divides $\varphi(N)$.

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

By considering the powers of 2 modulo N, you see that

$$2^p \equiv 1 \pmod{N}.$$

Hence, the value of $2^N \bmod N$ depends only on the value of N modulo p and is equal to 2^a where a is the least residue of $N \bmod p$. But by Fermat's little theorem,

$$N = 2^p - 1 = 2 - 1 = 1 \pmod{p}.$$

Hence

$$2^N - 2 = 2^1 - 2 = 0 \pmod{N},$$

as was to be shown.

7. Let $N = 2^{2^5} + 1$. Find an integer a such that $a^2 \equiv 1 \pmod{N}$ but such that $a \neq \pm 1 \pmod{N}$.
The key idea here was to use the factorisation of $N = pq$ into a product of two primes, and then, to use the Chinese remainder theorem to find an a which is congruent to 1 mod p and congruent to -1 mod q. This a will have the sought-for properties.

8. Simplify the expression $\phi(1) + \phi(2) + \cdots + \phi(n)$, where ϕ is the Euler ϕ-function. Deduce a simple formula (in terms of n) for the number of fractions a/b in lowest terms satisfying $1 \leq a < b \leq n$.
This question was an embarassing mistake on my part. I was thinking of the well-known fact that

$$\sum_{d|n} \phi(d) = n.$$

As far as I know, there is no simple formula for $\phi(1) + \cdots + \phi(n)$. Mea maxima culpa!

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.)

This is a direct consequence of Hensel's lemma.

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

$$C = 14572353050570834605889731500015117386453891958889990$$

encoded with the RSA public key

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

Knowing that the prime factorization of n is pq, where

$$p = 14732265321145317331353282383, \quad q = 11556853952466191826730 33,$$

find the secret message M. (Caveat: In the course of your calculation, you will need to compute $x^y \bmod z$, 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.
The idea here is to allow the remainder at the nth stage after division by b_n to be possibly negative, but less than $|b_n/2|$ *in absolute value.*

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?