189-346/377B: Number Theory

Assignment 3

Due: Monday, February 14

1. Solve *completely* the following congruence equations. More precisely, given the equation $f(x) \equiv 0 \pmod{N}$, list all the solutions between 0 and $N-1$. (You may use a computer to help yourself with the intermediate calculations if they get too lengthy, but you should justify the steps of the calculation.)

a) $x^2 + 1 \equiv 0 \pmod{493}$.

b) $x^3 - 1 \equiv 0 \pmod{13^5}$.

2. List all the primitive roots modulo $p = 17$ and modulo $n = 27$.

3. Let g be the smallest positive integer that is a primitive root modulo 17. Compute the value of g, and the mod 17 discrete logarithm $\log_g(12)$. Be sure to specify to which set this discrete logarithm belongs to.

4. In Pari, the expression `Mod(a,N)` denotes the residue class of a modulo N. The following Pari routine ("ft" stands for "Fermat Test")

```
ft(N,a) = Mod(a^N-a,N)
```

therefore implements the Fermat primality test for N, returning the object `Mod(0,N)` precisely when N is a pseudo-prime for the base a.

Type this function into Pari and use it to verify that 1105, 2821, and the fourth Fermat number $F_4 := 2^{2^4} + 1$ are pseudo-prime to the base 2, 3 and 5.

5. Try to use the function `ft` of exercise 4 to show that the 5-th and 6-th Fermat numbers F_5 and F_6 are composite. What happens? Explain why your program failed, and fix it so that it will work on these larger examples. Use your modified program to check that the Fermat numbers $F_n = 2^{2^n} + 1$ are composite for $5 \leq n \leq 12$ by showing that they are not strong pseudo-primes. For each N whose compositeness you are testing for, you should give the value of the base a that you use, and write out the first and last three digits of $a^N - a$ modulo N.

6. What happens in Exercise 5 when you try to show that F_n is composite by applying to it the Fermat test with the base $a = 2$? Give a proof (valid for all n) of your empirical observation.

7. Show that the integer n is a strong pseudo-prime (or a Carmichael number) if and only if the facotrisation of n is of the form

$$n = p_1 \cdots p_t,$$

where the p_j are *distinct* prime factors with the property that $p_j - 1$ divides $n - 1$ for all $1 \leq j \leq t$.

8. Show that the sequence (a_n) of integers given by

$$a_n = 1 + p + p^2 + p^3 + \cdots + p^n$$

converges in $\mathbf{Q}_p$, and that its limit is in fact a *rational number*, by computing the limit, a. Same question for the sequence

$$b_n = 1 + p + 2p^2 + 3p^3 + \cdots + np^n.$$

(Remark: most elements of $\mathbf{Q}_p$ or $\mathbf{Z}_p$ are irrational, and even transcendental, so the fact that a_n and b_n converge to a rational number represents "atypical" behaviour in some sense. As we will see towards the end of the course, the p-adic number

$$1 + p + p^2 + p^6 + p^{24} + \cdots + p^{n!} + \cdots$$

is transcendental, for example...)

* 9. In order to transmit its diplomatic cables via an RSA scheme, the US State Department decides to use the integer

$$\begin{aligned}&26456455855697905144088346504668395137052272600420492248344458\\&56405766479429811456937069928214101434215166632674854474518209 5\\&46797122926873145170157106347698033586399713543279394460142197\\&845732668752351513361 3,\end{aligned}$$

a product of three fairly large primes, as its RSA modulus. Julian Assange has just learned through one of his informants that $\phi(n)$ is equal to

$$\begin{aligned}&26456455855697905144088346504668395137052272600420492248344388 6\\&37978475018275704776484550828422131585782681050018190669858326 8\\&92134970479232644059688173549789734914853713441804381582562943 5\\&09414566747635778400,\end{aligned}$$

where ϕ denotes the Euler phi-function. Explain how this information could be exploited by Wikileaks to decipher the State Department's secret cables, and *give the prime factorisation of* n.

Hint. You will need to use Pari for this, but the computer calculation that you carry out should not be lengthy and requires no programming. Also, you may prefer to cut and paste the above numbers into your Pari session from an electronic copy of this assignment, rather than entering them by hand!...

Note. This is of course a made-up example. In "real life", the RSA standard calls for a public key that is about 1024-bit, or roughly 300 decimal digits, long, and is typically a product of two (rather than three) large primes.

* 10. Let a_n be the sequence of rational numbers given recursively by the formula

$$a_1 = 2, \qquad a_{n+1} = \frac{1}{2}(a_n - 1/a_n).$$

Show that the numerator of the rational number $a_n^2 + 1$ (in lowest terms) is divisibly by 5^n. Use this to show that (a_n) is a Cauchy sequence relative

to the 5-adic metric on $\mathbf{Q}$, and that it converges in $\mathbf{Q}_5$ to a square root of -1. (This exercise shows that the complex number i is less mysterious in the 5-adic world than in the Archimedean world.)