189-346/377B: Number Theory
Assignment 3

Due: Monday, February 14

1. Find the remainder in the division of $3^{10000001}$ by 707, i.e., the unique $r \in \mathbf{Z}$ such that

$$3^{10000001} = 707q + r, \quad 0 \leq r \leq 706.$$

2. 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) $x^2 + 1 \equiv 0 \pmod{65}$.

b) $x^3 + x + 1 \equiv 0 \pmod{11^5}$.

3. Let p be an odd prime, let a be an integer, and let d be an exponent which is not divisible by p, for which

$$a^d \equiv 1 \pmod{p}.$$

Show that the sequence (a^{p^n}) is a Cauchy sequence in $\mathbf{Q}_p$ which converges p-adically to a root of the polynomial $x^d - 1$, and moreover that all roots of this polynomial are given in this way. Conclude that the number of distinct roots of the polynomial $x^d - 1$ in the field $\mathbf{Q}_p$ of p-adic numbers is equal to $\gcd(d, p-1)$.

4. List all the primitive roots modulo $p = 37$ and modulo 25.

5. Let g be the smallest positive integer that is a primitive root modulo 37. Compute the value of g, and the mod 37 discrete logarithm $\log_g(12)$.

6. Let p be an odd prime. Let j be an element of $\mathbf{Z}/p\mathbf{Z}$, and consider the polynomials in $\mathbf{Z}/p\mathbf{Z}[x]$, depending on a parameter $j \in \mathbf{Z}/p\mathbf{Z}$ and defined by

$$f_j = (x-j)^{\frac{p-1}{2}} - 1, \qquad g_j = (x-j)^{\frac{p-1}{2}} + 1.$$

Show that

$$x^p - x = (x - j) f_j(x) g_j(x).$$

Conclude that the roots of f_j and g_j are disjoint subsets A_j and B_j of $\mathbf{Z}/p\mathbf{Z}$ satisfying

$$A_j \cup B_j = \mathbf{Z}/p\mathbf{Z} - \{j\}.$$

Give a simple description of A_j and B_j.

7. Find the roots of the equation

$$f(x) = x^3 - 432157053 * x^2 - 340972635592 * x + 42461236607868$$

modulo the prime 982451653 by calculating the *gcd* of $f(x)$ and $x^{982451653} - x$ with Pari.

Hint. It is easy to launch the calculation in the wrong way and ask Pari to do something impossibly long. You will know you started on the wrong foot if your calculation takes more than 1 or 2 seconds. In that case it will probably not end in a billion years, or you will get a stack overflow before that.

The following Pari commands may come in handy to avoid these potential pitfalls.

- The command `Mod(n,p)` creates a PARI object which is the residue class of n mod p. Arithmetic operations on this object will always be performed mod p.
- The command `Mod(f(x),g(x))` will create a PARI object which is the residue class of the polynomial $f(x)$, taken modulo the polynomial $g(x)$.
- PARI is perfectly happy to work with expressions like

  $$\texttt{Mod(5,7)} * \texttt{x}^2 - \texttt{Mod(4,7)}$$

  which is how you would want to represent a polynomial with entries in $\mathbf{Z}/7\mathbf{Z}$.

The following problems are optional for Math 346

8. In order to transmit its diplomatic cables, the US state department decides to use the integer

$$n = 1412364903523718702627683835801071363307551539748828\,6$$

$$5074356572388972394874625465333820363740152221,$$

a product of two fairly large primes of roughly equal size, as the public key in its RSA cryptosystem. Julian Assange has just learned that one of the prime factors of n is of the form $1 + k$, where k is only divisible by primes that are less than 50. Explain why this is good news for Wikileaks, 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.

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 it is also common practice to avoid using primes p for which $p - 1$ is divisible only by small primes!

9. Using the notations of Problem 6, show that for any polynomial $h(x)$ in $\mathbf{Z}/p\mathbf{Z}[x]$,

$$\gcd(h(x), f_j(x)) = \prod_{\substack{a \in A_j \\ h(a)=0}} (x - a), \quad \gcd(h(x), g_j(x)) = \prod_{\substack{b \in B_j \\ h(b)=0}} (x - b).$$

Assuming that $h(x)$ has r distinct roots in $\mathbf{Z}/p\mathbf{Z}$, and following the heuristic that (A_j, B_j) is, as j varies, a "random" partitioning of $\mathbf{Z}/p\mathbf{Z}$ into disjoint subsets of equal size, estimate the likelihood that both these factors of $h(x)$ are different from 1 when j is chosen at random.

10. Use what you've learned in the previous problem to compute the square root of 3 modulo the prime

$$p = 29927402397991286489627837734179186385188296382227$$

Note. Pari will allow you to do this with a built-in command. Don't cheat! In particular you should explain the steps of the calculation you've carried out.