189-346/377B: Number Theory

Assignment 3

Due: Monday, February 12

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) $3x + 2 \equiv 0 \pmod{3^{11}}$.
b) $3x + 3 \equiv 0 \pmod{3^{11}}$.
c) $x^2 + 1 \equiv 0 \pmod{65}$.
d) $x^3 + x + 1 \equiv 0 \pmod{11^5}$.

3. Show that the polynomial $x^d - 1$ has a root in the field $\mathbf{Q}_p$ of p-adic numbers if and only if d divides $(p-1)$, and that in that case, the polynomial $x^d - 1$ has d distinct roots in $\mathbf{Q}_p$.

4. 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.

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

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

7. Let a be an element of order t in $(\mathbf{Z}/p\mathbf{Z})^\times$. Show that $a + a^2 + \cdots + a^{t-1} = -1$ in $\mathbf{Z}/p\mathbf{Z}$.

8. Let g be a primitive root modulo an odd prime p. Show that $-g$ is also a primitive root modulo p if and only if 4 divides $p - 1$.

9. Let p be an odd prime. Show that, for all $N \geq 1$,

$$(1 - 2p) = (1 - p)^j \pmod{p^N},$$

where

$$j = \frac{(2p) + (2p)^2/2 + (2p)^3/3 + \cdots + (2p)^N/N}{p + p^2/2 + p^3/3 + \cdots + p^N/N}.$$

Can you formulate this as an identity between p-adic numbers?

The following problems are optional for Math 346

10. Using the notations of Problem 4, show that for any polynomial $h(x)$ in $\mathbf{Z}/p\mathbf{Z}[x]$,

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

Given that $h(x)$ has r distinct roots in $\mathbf{Z}/p\mathbf{Z}$, and that j is chosen at random, estimate the likelihood that both these factors of $h(x)$ are different from 1.

11. Using the outcome of problems 4 and 10, describe an *efficient* probabilistic algorithm for finding the roots of a polynomial over $\mathbf{Z}/p\mathbf{Z}$.