189-346/377B: Number Theory

Assignment 3

Corrections

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

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

Solution. Since $10000001 \equiv 5 \pmod 6$, it follows that

$$3^{10000001} \equiv 3^5 \equiv 5 \pmod 7,$$

while, by a similar argument

$$3^{10000001} \equiv 3^1 \equiv 3 \pmod{101}.$$

Now, it follows from the Chinese remainder theorem that

$$3^{10000001} \equiv 306 \pmod{707}.$$

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

Solution. a) You can solve the equation modulo 5 and 13 seperately; each of these equations has two distinct roots mod 5 and 13 respectively. Now invoke the Chinese remainer theorem, to get a total of *four* possible roots modulo 65.

b) There is a single root of this equation modulo 11, namely, 2. Now, to find the root modulo 11^5, use Hensel's Lemma.

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 $\gcd(d, p-1)$.

Soution. If $M \leq N$ are (large) integers, then the difference

$$a^{p^M} - a^{p^N} = a^{p^M}(1 - a^{p^N - p^M}) = a^{p^M}(1 - a^{p^M(p^{N-M}-1)}) = a^{p^M}(1 - b^{p^M}),$$

where $b = a^{p^{N-M}-1}$. But note that, since $p-1$ divides $p^{N-M}-1$, the integer b is necessarily congruent to 1 modulo p. By what we have seen in class,

$$b^{p^M} \equiv 1 \pmod{p^{M+1}},$$

so that p^{M+1} divides $1 - b^{p^M}$, and therefore $a^{p^M} - a^{p^N}$. Therefore

$$|a^{p^M} - a^{p^N}|_p \leq p^{-M}.$$

In particular, for any real $\epsilon > 0$, it suffices to choose an integer $B > 0$ for which $p^{-B} < \epsilon$ to ensure that

$$|a^{p^M} - a^{p^N}|_p \leq \epsilon, \quad \text{for all } M, N > B.$$

It follows that the sequence a^{p^n} is a Cauchy sequence.

To see that this Cauchy sequence converges to a dth root of unity, note that $(a^{p^n})^d = c^{p^n}$ with $c = a^d \equiv 1 \pmod{p}$. Therefore $c^{p^n} \equiv 1 \pmod{p^{n+1}}$ and it follows that the sequence $(a^{p^n})^d$ converges to 1 in the p-adic metric, as was to be shown.

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

Solution. A direct calculation. Note that there are $\varphi(\varphi(37)) = \varphi(36) = 12$ primitive roots modulo 37, and $\varphi(20) = 8$ primitive roots 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 $\log_g(12)$.

Solution. This integer is $g = 2$, and the discrete log of 12 to the base g is 28 (mod 36).

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.

Solution. The key point is that the sets A_j (resp. B_j) of roots of f_j (resp. g_j) are precisely the elements r of $\mathbf{Z}/p\mathbf{Z}$ for which $r - j$ is a non-zero quadratic residue (resp. non-residue) modulo p. It follows that

$$\{1, \ldots, p-1\} = A_j \cup B_j \cup \{j\},$$

in which the union above is a *disoint union.* The identity

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

follows directly from this after noting that the polynomials on both sides ave the same p distinct roots and have the same leading coefficient of one.

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 $\mathbf{Z}/7\mathbf{Z}$.

Solution. The unique root is 432157842, as shown by the following PARI dialogue. (The computer output is in regular characters, and the input I've typed in is in boldface).

? **p = 982451653**

%1 = 982451653

? **f= x^3 - Mod(432157053,p)*x^2 - Mod(340972635592,p)*x + Mod(42461236607868,p)**

%2 = x^3 + Mod(550294600, 982451653)*x^2 + Mod(920539652, 982451653)*x + Mod(658616861, 982451653)

? **g= Mod(x,f)^p-x**

%3 = Mod(Mod(426137915, 982451653)*x^2 + Mod(224349607, 982451653)*x + Mod(369846355, 982451653), x^3 + Mod(550294600, 982451653)*x^2 + Mod(920539652, 982451653)*x + Mod(658616861, 982451653))

? **gcd(f,g)**

%4 = Mod(Mod(387231511, 982451653)*x + Mod(870854745, 982451653), x^3 + Mod(550294600, 982451653)*x^2 + Mod(920539652, 982451653)*x + Mod(658616861, 982451653))

? **r = - 870854745/ 387231511 % p**
%5 = 432157842
? **x=r**
%6 = 432157842
? **eval(f)**
%7 = Mod(0, 982451653)

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

$$n = 14123649035237187026276838358010713633075515397488286$$
$$5074356572388972394874625465333820363740152221,$$

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!

Solution. The idea is that, if $n = pq$ and $p - 1$ is divisible only by primes < 50, and a is any integer, then, after letting M be the product of all p less than 50, raised to a suitable large power ($[log_p n]$ will do, or you can just take the power to be 400, which is overkill, but easier to program), we will have

$$b := a^M \equiv 1 \pmod{p}.$$

Of course, this number is huge, but it is enough to compute it mod n. One can then recover the prime p by calculating $\gcd(b-1, n)$. This method of factoring large integers is called the *Pollard $p-1$* method. Its scope is severely restricted by the fact that the integer n to be factored has to have a prime divisor p for which $p-1$ is only divisible by "small" primes. (A number with this property is called a *smooth number*, or a *nombre friable* in the more sugestive french terminology.)

Here is a sample PARI script that factors n by the Pollard approach.

```
? n = 14123649035237187026276838358010713633075515397488286507435657238897239487462546533382036374015222 1;
? a = Mod(2,n);
? P = primes(15)
%1 = [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47]
? for(j=1,15, p = P[j]; a= a^(p^400))
? a
%2 = Mod(10382245446865264567580379861832535504091234264291656
   30143825494051016330937460525756507051864440 0,
   14123649035237187026276838358010713633075515397488286507435657238897239487462546533382036374015222 1)
? A = component(a,2)
%3 = 10382245446865264567580379861832535504091234264291656
   30143825494051016330937460525756507051864440 0
? p = gcd(A-1,n)
%4 = 39305063412410223286956703455542737154290483 3
? q = n/p
%5 = 35933408596862283104196018859804366106538872695907983 7
? isprime(p)
%6 = 1
? isprime(q)
%7 = 1
? n-p*q
%8 = 0
```

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.

Solution. Each of the sets A_j and B_j has size $(p-1)/2$. If p is large, the probability that any of the roots would be equal to j is negligible, and the probability that all r roots would fall in A_j is roughly $(1/2)^r$. Hence the probability that al roots would lie in either A_j or B_j is $(1/2)^{r-1}$, which is always less than a half, as soon as $r > 1$. (If $r = 1$, of course, there is nothing to do...) So one can hope to factor $h(x)$ probabilistically by varying j at random and computing $\gcd(h(x), f_j(x)$. For any given j this might fail to produce a non-trivial factorisation, but the probability of failure at each trial is less than 50%, and hence the probability of failure after (say) 30 repeated trials would be very small indeed. Such a probabilistic approach, while not completely satisfying in theory, works very well in practice and a lot of number theoretic problems admit efficient probabilistic solutions of this sort.

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.
Solution. Here is a simple PARI script to extract the square root of 3 mod p using probabilistic methods.

? **p = 29927402397991286489627837734179186385188296382227;**

? **X = Mod(x, x^2-Mod(3,p));**
? **X$^{((p-1)/2)}$-1**
%3 = Mod(Mod(1328586973614502501762054658609980693238250612859 1,
2992740239799128648962783773417918638518829638222 7)*x - 1,
x^2 + Mod(2992740239799128648962783773417918638518829638222 4,
2992740239799128648962783773417918638518829638222 7))
? **a = 1/1328586973614502501762054658609980693238250612859 1**
% p
%4 = 9930206810443788563233802024120234411959222003546
? **a^2 % p**
%5 = 3

Note that, in this calculation, the first try, with the natural value of $j = 0$, already worked. This was because 3 has a *unique* square root mod p that is a quadratic residue modulo p. You might try to think about the primes for which this happens. (And, this question will be pursued in assignment 4...)