189-346/377B: Number Theory
Corrections to assignment 4

1. Solve the equation

$$6^x = 11 \pmod{5^{12}}$$

by using the power series expansion for the logarithm, as seen in class. Some of this calculation is a bit tedious so you may want to do it on the computer. Check that the value of x you obtain is the correct one by computing 6^x (mod 5^{12}) directly.

Solution: This is an exercise in calculating p-adic logarithms (for $p = 5$). Indeed, by what we saw in class we know that

$$x = \frac{\log(1+10)}{\log(1+5)} = \frac{10 - 10^2/2 + 10^3/3 - \cdots + 10^{11}/11 - \cdots}{5 - 5^2/2 + 5^3/3 - \cdots + 5^{11}/11 - \cdots}.$$

Since we are only interested in the value of x modulo 5^{11}, we can neglect all terms in numerator and denominator that involve 12th powers or more – but *not* 11th powers, because the denominator in the ratio of logarithms is divisible by 5, exactly once! This is the main subtlety to keep into acount. If you calculate numerators and denominators modulo 5^{11} seperately, and then perform the division, you will get a wrong answer.

With this caveat, the following Pari dialogue shows that $x = 29342597$ is the right answer.

```
? num = sum(j=1,11,(-1)^(j+1)*10^j/j)
%1 = 5676224330780/693
? den = sum(j=1,11,(-1)^(j+1)*5^j/j)
%2 = 20177960045/5544
? x = num/den
%3 = 9081958929248/4035592009
? x = x % (5^11)
```

```
%4 = 29342597
? Mod(6,5^12)^x
%5 = Mod(11, 244140625)
```

2. Show that 10^{101^j} converges to a square root of -1 in the field $\mathbf{Q}_{101}$ of 101-adic numbers.

Solution: This is very similar to a problem that was already given in last week's assignment.

3. Show that, if $\zeta = e^{(2\pi i)/5} = \cos 2\pi/5 + i \sin 2\pi/5$ is the primitive 5th root of unity, and if $\omega = \frac{-1+\sqrt{5}}{2}$ is the golden ratio, then

$$\zeta + \zeta^{-1} = \omega.$$

Use this to show that, if p is an odd prime, the Legendre symbol $(\frac{5}{p})$ is equal to 1 if and only $p \equiv \pm 1 \pmod 5$.

Solution. For the first part, if we set $x = \zeta + \zeta^{-1}$, then we have

$$x^2 = \zeta^2 + \zeta^{-2} + 2, \quad x^2 + x = \zeta + \zeta^{-1} + \zeta^2 + \zeta^{-2} + 2 = 1,$$

where the last equality follows from the fact that the sum of the four distinct primitive 5th roots of unity is equal to $= 1$. Hence $\zeta + \zeta^{-1}$ satisfies the quadratic equation $x^2 + x - 1 = 0$, and is > 1, therefore it is equal to ω.

For the second part of the problem, we can proceed by calculating $\omega^p \pmod p$ in two different ways, exactly as was done in class for the case of $\omega = \frac{\sqrt{2}+\sqrt{-2}}{2} = \zeta_8$.

4. Let p be a prime which is congruent to 3 modulo 4. Show that the square root of a mod p, if it exists, is equal to $a^{\frac{p+1}{4}}$. Conclude that there is a polynomial time algorithm (in $\log(p)$) for calculating square roots mod p.

Solution: This follows from the fact that

$$(a^{\frac{p+1}{4}})^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} a = \left(\frac{a}{p}\right) a.$$

The polynomial time algorithm for calculating the square root of a mod p proceeds by calculating $a^{\frac{p+1}{4}}$ by the method of successive squaring which requires roughly $\log p$ multiplications in $\mathbf{Z}/p\mathbf{Z}$.

5. Evaluate the Legendre symbols $(\frac{503}{773})$ and $(\frac{501}{773})$ using the law of quadratic reciprocity.

Solution. A direct calculation shows that

$$\begin{aligned}(\frac{503}{773}) &= (\frac{773}{503}) = (\frac{270}{503}) = (\frac{30}{503}) = (\frac{2}{503})(\frac{3}{503})(\frac{5}{503}) \\ &= 1 \times -(\frac{503}{3}) \times (\frac{503}{5}) = 1 \times 1 \times (-1) = -1.\end{aligned}$$

The calculation for $(\frac{501}{773})$ is similar.

6. Decide (by hand, without a computer!) which of the following congruences have a solution:

a) $x^2 \equiv 2455 \pmod{4993}$;
b) $1709x^2 \equiv 2455 \pmod{4993}$;
c) $x^2 \equiv 245 \pmod{27496}$;
d) $x^2 \equiv 5473 \pmod{27496}$;

Try your hand at solving the congruence equations (either by hand, or, if you get tired, by computer.)

Solution. The relevant Legendre or Jacobi symbols can be calculated by repeated applications of quadratic reciprocity, as in the previous exercise.

7. If n is an integer that is prime to 3, show that the all the odd primes dividing $n^2 + 3$ are congruent to 1 modulo 3. Use this to show that there are infinitely many primes of the form $3k + 1$.

Solution. If an odd prime p divides $x^2 + 3$, then x is a square root of -3 modulo p, and hence $p \equiv 1 \pmod{3}$ by quadratic reciprocity. To conclude that there are infinitely primes of this form, one can argue by contradiction, and assume that there are only k such primes, $p_1, \ldots, p_k$. Then it would follow that every integer of the form $n^2 + 3$ is of the form $p_1^{e_1} \cdots p_k^{e_k}$. But the number of such integers that are less than X is bounded by a constant multiple of $(\log X)^k$, since each exponent e_j must be less than $\log(X)/\log(p_j)$. On the other hand, the number of integers less than X that are of the form n^2+3 is roughly $\sqrt{X}$. This is a contradiction, since $\sqrt{(X)}$ grows faster than any power of $\log(X)$.

For Math 377 students only.

8. What can you say about exercise 4 when $p \equiv 1 \pmod 4$?

Solution. This was an open-ended question, whose main purpose was to make you realise that the method used in exercise 4 breaks down in this case. The most natural generalisation, which works when $p = 5 \pmod 8$, is to consider the expression $a^{\frac{p+3}{8}}$, whose square is $a^{\frac{p+3}{4}} = a^{\frac{p-1}{4}}a$. This produces a square root of a when a is a *fourth power* modulo p, and a square root of $-a$ when a is a square but not a fourth power. So this leads to a polynomial time algorithm for extracting square roots mod p for certain a, but a completely general algorithm for extracting square roots in polynomial time, in a completely deterministic way, is an interesting problem that has led to a lot of research in number theory. For a brief summary of the main facts, and some references, see
`http://en.wikipedia.org/wiki/Quadratic_residue`
`#Complexity_of_finding_square_roots`

9. Let a be an element of $(\mathbf{Z}/p\mathbf{Z})^\times$, and view the function $x \mapsto ax$ as a permutation on the $p-1$ elements in $(\mathbf{Z}/p\mathbf{Z})^\times$. Show that this permutation is even if $(\frac{a}{p}) = 1$, and is odd if $(\frac{a}{p}) = -1$. (This statement is known as Zolotarev's lemma.)

Solution. This problem is easier than I thought when I posed it (provided you are comfortable with the notion of the sign of a permutation, which you learn in a first course in group theory.) Indeed, the permutation σ attached to a primitive root g is just a single cycle of length $p-1$, and hence is an odd permutation since $p-1$ is even. Now, if $a = g^e$ is any element of $\mathbf{Z}/p\mathbf{Z}^\times$, its associated permutation is σ^e, which is even if e is even, and odd if e is odd. But the former holds if a is a quadratic residue, and the latter, if a is a quadratic non-residue.

10. Can Hensel's lemma, which is used to solve equations of the form $f(x) = 0$ over the p-adic numbers when f is a polynomial, be extended to the setting where f is a *power series* with rational coefficients? Discuss. Use what you have learned to solve the equation

$$x + \log(x) = 4 \pmod{3^{10}}$$

numerically (on the computer). (Here $\log(x)$ refers to the 3-adic logarithm, which is given on $1 + 3\mathbf{Z}$ by the formula

$$\log(1+t) = \sum_{j=1}^{\infty} (-1)^{j+1} t^j / j.)$$

Solution. Newton iteration works just as well with analytic functions (given locally by a power series expansion) as it does for polynomials. The proof of Hensel's lemma given in class allowing the solution of $f(x) = 0$ extends directly to the setting where $f(x)$ is a power series rather than a polynomial, the only difference being that the expansion of $f(x)$ about the root is an infinite (but still onvergent!) sum rather than a finite one.

To solve the equation

$$f(x) := x + \log(x) - 4 = 0 \pmod{3^{10}},$$

we observe first that

$$f(1) = -3 \equiv 0 \pmod 3, \qquad f'(1) = 1 + 1 = 2 \neq 0 \pmod 3,$$

hence we are in a good position to apply Hensel's lemma, starting with the "initial approximation" $r_0 = 1$, and making the recursive substitution

$$r_{n+1} = r_n - \frac{r_n + \log(r_n) - 4}{1 + 1/r_n}.$$

The following dialogue in Pari illustrates how this is done in practice:

```
? r = 1+ O(3^10)
```

```
%1 = 1 + O(3^10)
? for(j=1,4, r = r -(r+log(r)-4)/(1+1/r))
? r
%2 = 1 + 2*3 + 3^2 + 3^3 + 3^5 + 2*3^6 + 3^9 + O(3^10)
? r+log(r)
%3 = 1 + 3 + O(3^10)
```

The pedagogical purpose of this exercise was to make you appreciate more fully the analytic nature of p-adic numbers. The above PARI dialogue also illustrates how p-adic numbers can be handled computationally. Note that in the dialogue above, only four iterations were performed, to obtain the solution modulo 3^{10}. Can you justify why this is enough? (Of course, any larger number of iterations would have worked fine, as well.)

Note also that the way in which I have handled p-adic numbers in this solution is more efficient than the way they were handled in exercise 1, where I did not make use of the p-adic logarithm function that is built into PARI, but programmed it myself. You might want to revisit the solution to exercise 1, using the more powerful commands in PARI that are illustrated in my solution to exercise 10.