Math 261 — Exam 2

November 7, 2018

The use of notes and books is **NOT** allowed.

Exercise 1: Polynomials mod 691 (30 pts)

In this exercise, you may freely use the fact that 691 *is* ***prime****.*

Consider the polynomials $f(x) = x^4 + 4x^3 + 4x^2 - 5x - 12$ and $g(x) = x^2 + 3x + 4$ in $(\mathbb{Z}/691\mathbb{Z})[x]$.

1. (5 pts) Check that $g(x) \mid f(x)$, and find a polynomial $h(x)$ such that $f(x) = g(x)h(x)$.
2. (5 pts) State the law of quadratic reciprocity.
3. (16 pts) Use Legendre symbols to prove that neither $g(x)$ nor $h(x)$ have any roots in $\mathbb{Z}/691\mathbb{Z}$.
4. (4 pts) What is the complete factorization of $f(x)$ in $(\mathbb{Z}/691\mathbb{Z})[x]$?

   Make sure to justify that your factors are irreducible.

Solution 1:

1. By performing the Euclidean division of $f(x)$ by $g(x)$, we find quotient x^2+x-3 and remainder 0. So we can (and must) take $h(x) = x^2 + x - 3$.
2. Let p and q be distinct, odd primes. Then
$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right).$$
3. For $g(x)$, we have $\Delta = -7$. We compute that
$$\left(\frac{-7}{691}\right) = \left(\frac{-1}{691}\right)\left(\frac{7}{691}\right) = -1 \times -\left(\frac{691}{7}\right)$$
by quadratic reciprocity and since $691 \equiv -1 \pmod 4$
$$= \left(\frac{-9}{7}\right) = \left(\frac{-1}{7}\right)\left(\frac{9}{7}\right) = \left(\frac{-1}{7}\right)$$
since $691 \equiv -9 \pmod 7$ and since $9 = 3^2$ is clearly a square mod 7
$$= -1$$
since $7 \equiv -1 \pmod 4$. This shows that $g(x)$ has not roots in $\mathbb{Z}/691\mathbb{Z}$.

For $h(x)$, we have $\Delta = 13$, and

$$\left(\frac{13}{691}\right) = \left(\frac{691}{13}\right) = \left(\frac{41}{13}\right) = \left(\frac{2}{13}\right)$$

by quadratic reciprocity and because $691 \equiv 41 \equiv 2 \pmod{13}$

$$= -1$$

since $13 \equiv \pm 3 \pmod 8$. So $h(x)$ has no root either.

4. If a polynomial of degree 2 is reducible, then it has a factor of degree 1, so it has a root. Therefore $g(x)$ and $h(x)$ are irreducible, and

$$f(x) = g(x)h(x)$$

is the complete factorization of $f(x)$.

Exercise 2: The Pépin test (30 pts)

In the 17th century, the French mathematician Pierre de Fermat studied the numbers

$$F_n = 2^{2^n} + 1,$$

where $n \in \mathbb{N}$. The purpose of this exercise is to establish a criterion to test whether F_n is prime. In the rest of the exercise, we fix $n \in \mathbb{N}$.

1. (4 pts) Prove that $F_n \equiv -1 \pmod 3$ and that $F_n \equiv 1 \pmod 4$.
2. (4 pts) Let $p \in \mathbb{N}$ be a prime such that $p \equiv 1 \pmod 4$. Prove that $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$.
3. (7 pts) Use the previous questions to prove that if F_n is prime, then

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}.$$

4. (15 pts) Conversely, prove that if $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$, then F_n is prime. *Hint: Square both sides. What is $F_n - 1$, and what does this tell you about the multiplicative order of* 3 mod F_n*?*

Solution 2:

1. Since $2 \equiv -1 \pmod 3$, we have

$$F_n = 2^{2^n} + 1 \equiv (-1)^{2^n} + 1 = 1 + 1 = 2 \equiv -1 \pmod 3$$

as $n \geqslant 1$. Besides, $2^n \geqslant 2^1 = 2$ so 2^{2^n} is a multiple of 4, whence $F_n = 2^{2^n} \equiv 1 \pmod 4$.

2. This is an immediate consequence of quadratic reciprocity.

3. If $F_n = p$ is prime, then we have $3^{(F_n-1)/2} = 3^{p'} \equiv \left(\frac{3}{p}\right) \pmod p$, and $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ by the previous question since clearly $p = F_n \equiv 1 \pmod 4$. Since $F_n \equiv -1 \pmod 3$, $\left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1$, whence the result.

4. If $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$, then $3^{F_n-1} \equiv (-1)^2 = 1 \pmod{F_n}$, so the multiplicative order of 3 mod F_n divides $F_n - 1 = 2^{2^n}$, which is a power of 2. Since $3^{(F_n-1)/2} \equiv -1 \not\equiv 1 \pmod{F_n}$, and since 2 is the only prime dividing $F_n - 1$, this order is in fact exactly $F_n - 1$. So the powers of 3 give us $F_n - 1$ elements in $(\mathbb{Z}/F_n\mathbb{Z})^\times$. But the number of elements in $(\mathbb{Z}/F_n\mathbb{Z})^\times$ is at most $F_n - 1$ since 0 is not invertible, so the powers of 3 give us all of $(\mathbb{Z}/F_n\mathbb{Z})^\times$ (i.e. 3 is a primitive root mod F_n) and all nonzero elements in $\mathbb{Z}/F_n\mathbb{Z}$ are invertible. This means that $\mathbb{Z}/F_n\mathbb{Z}$ is a field, which implies that F_n is prime.

Remark: Fermat noticed that F_n is prime for $n \leqslant 4$, and claimed that F_n was actually prime for every n. Euler later showed that this was not true, since for instance $F_5 = 641 \times 6700417$.

The primality test presented in this exercise is named after the 19th century French mathematician Théophile Pépin. It only applies to Fermat numbers, but is much faster than the general-purpose tests that can deal with any integer. It was used in 1999 to prove that F_{24} is composite, which is quite an impressive feat since F_{24} has 5050446 digits!

It is know today that F_n is composite for all $5 \leqslant n \leqslant 32$. Proving that Fermat was totally wrong, in other words that F_n is never prime when $n \geqslant 5$, is still an open problem; in fact, as of today it is not known whether the 2585827973-digit number F_{33} is prime.

Exercise 3: The Solovay-Strassen test (40 pts)

In this exercise, we fix an **odd** integer $N \geqslant 3$, **not** necessarily prime. Let

$$N = \prod_{i=1}^{r} p_i^{v_i}$$

be its factorization, where the p_i are distinct primes. We **define** the Jacobi symbol by the formula

$$\left[\frac{x}{N}\right] = \prod_{i=1}^{r} \left(\frac{x}{p_i}\right)^{v_i} \in \mathbb{Z}$$

for all $x \in \mathbb{Z}$, where $\left(\frac{x}{p_i}\right)$ is the usual Legendre symbol defined in class. In particular, if N is prime, then $\left[\frac{x}{N}\right] = \left(\frac{x}{N}\right)$.

1. In this question, we investigate some basic properties of the symbol $\left[\frac{x}{N}\right]$.

   The sub-questions of this question are independent from each other.

   (a) (3pts) Prove that if $x \equiv y \pmod{N}$, then $\left[\frac{x}{N}\right] = \left[\frac{y}{N}\right]$.

   (b) (6 pts) Prove that $\left[\frac{x}{N}\right] \neq 0 \iff x$ is invertible mod N.

   (c) (3 pts) Prove that $\left[\frac{xy}{N}\right] = \left[\frac{x}{N}\right]\left[\frac{y}{N}\right]$.

   We now introduce the function

$$\begin{array}{rccc} S: & (\mathbb{Z}/N\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/N\mathbb{Z})^\times \\ & x & \longmapsto & \left[\frac{x}{N}\right] x^{\frac{N-1}{2}}. \end{array}$$

2. (10 pts) Prove that if N is prime, then $S(x) = 1$ for all $x \in (\mathbb{Z}/N\mathbb{Z})^\times$.

3. The goal of this question is to prove that conversely, if N is not prime, then $S(x)$ is not always 1.

   In order to make things easier, we will suppose that N is composite and ***squarefree****, that is to say that $N = p_1 p_2 \cdots p_r$ with the p_i distinct primes and $r \geqslant 2$. We* ***define*** *$M = N/p_1 = p_2 \cdots p_r$.*

   (a) (10 pts) Prove that there exists a $t \in \mathbb{Z}$ such that $\left(\frac{t}{p_1}\right) = -1$ and that $t \equiv 1 \pmod{M}$.
   Hint: CRT.

   (b) (8 pts) Prove that if t is as in the previous question, then $S(t) \neq 1$.
   Hint: Compute $S(t)$ mod M.

Solution 3:

1. (a) If $x \equiv y \pmod{N}$, then $x \equiv y \pmod{p_i}$ for all i, and therefore $\left(\frac{x}{p_i}\right) = \left(\frac{y}{p_i}\right)$ for all i, so that $\left[\frac{x}{N}\right] = \left[\frac{y}{N}\right]$.

   (b) $\left[\frac{x}{N}\right] \neq 0 \iff \left(\frac{x}{p_i}\right) \neq 0$ for all $i \iff p_i \nmid x$ for all $i \iff \gcd(x, N) = 1$.

   (c) $$\left[\frac{xy}{N}\right] = \prod_{i=1}^{r} \left(\frac{xy}{p_i}\right)^{v_i} = \prod_{i=1}^{r} \left(\left(\frac{x}{p_i}\right)\left(\frac{y}{p_i}\right)\right)^{v_i} = \prod_{i=1}^{r} \left(\frac{x}{p_i}\right)^{v_i} \left(\frac{y}{p_i}\right)^{v_i}$$
   $$= \prod_{i=1}^{r} \left(\frac{x}{p_i}\right)^{v_i} \prod_{i=1}^{r} \left(\frac{x}{p_i}\right)^{v_i} = \left[\frac{x}{N}\right]\left[\frac{y}{N}\right].$$

2. If N is prime, then for all x, $\left[\frac{x}{N}\right]$ is simply $\left(\frac{x}{N}\right)$, which is congruent to $x^{\frac{N-1}{2}}$ mod N. Therefore, if $x \in (\mathbb{Z}/N\mathbb{Z})^\times$, then
   $$S(x) = x^{\frac{N-1}{2}} x^{\frac{N-1}{2}} = x^{N-1} = 1$$
   by Fermat's little theorem.

3. (a) Since N is odd, so is p_1, so we know that in $(\mathbb{Z}/p_1\mathbb{Z})^\times$, half of the elements are not squares. In particular, there exists $t_1 \in (\mathbb{Z}/p_1\mathbb{Z})^\times$ such that $\left(\frac{t_1}{p_1}\right) = -1$. Let also $t_2 = 1 \in \mathbb{Z}/M\mathbb{Z}$. Now p_1 and $M = p_2 \cdots p_r$ are coprime since the p_i are pairwise distinct, so by CRT we may find a $t \in \mathbb{Z}$ which reduces to t_1 mod p_1 and to $t_2 = 1$ mod M. This t solves the question.

   (b) By construction we have $\left(\frac{t}{p_1}\right) = -1$ whereas $\left(\frac{t}{p_i}\right) = \left(\frac{1}{p_i}\right) = +1$ for all $i \geqslant 2$, so
   $$\left[\frac{t}{N}\right] = \prod_{i=1}^{r} \left(\frac{t}{p_i}\right) = -1 \times +1 \times +1 \times +1 \times \cdots = -1.$$
   Besides, since $t \equiv 1 \bmod M$, we obviously have $t^{\frac{N-1}{2}} \equiv 1^{\frac{N-1}{2}} = 1 \pmod{M}$. As a result, we have
   $$S(t) \equiv -1 \times 1 = -1 \pmod{M}$$
   . If we had $S(t) \equiv 1 \pmod{N}$, then we would also have $S(t) \equiv 1 \pmod{M}$, so that $-1 \equiv 1 \pmod{M}$. Since $M = p_2 \cdots p_r > 2$, this is absurd, so $S(t) \not\equiv 1 \pmod{N}$.

Remark: The Jacobi symbol also obeys a form of quadratic reciprocity, which makes it easy to evaluate even if the factorization of N is unknown. Besides, we clearly have

$$x \text{ is a square mod } N \Longrightarrow \left[\frac{x}{N}\right] = +1$$

for all $x \in (\mathbb{Z}/N\mathbb{Z})^\times$; however, the converse is not true, so the Jacobi symbol is less powerful that the Legendre symbol.

Once can prove that there exists t such that $S(t) = 1$ even when N is not square-free. Besides, if such a t exists, then $S(x) \neq 1$ for "many" x. Indeed, consider

$$K = \{x \in (\mathbb{Z}/N\mathbb{Z})^\times \mid S(x) = 1\}.$$

One sees easily that for each $k \in K$, $S(tk) = S(t)S(k) = S(t) \times 1 \neq 1$; as a result, we can construct (at least) $\#K$ elements $x = tk \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $S(x) \neq 1$, which shows that the proportion of $x \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $S(x) \neq 1$ is $\geqslant 50\%$ (In more technical terms, this is just saying that since S is a non-trivial group homomorphism, its kernel has index at least 2). Therefore, by trying a few x at random, we will quickly find one such that $S(x) \neq 1$, and so we will be able to detect that N is not prime.

This test is thus useful to weed out composite numbers, but it cannot be used to prove rigorously that a number is prime. It has been superseded by the Rabin-Miller test, which suffers from the same limitation but is more efficient.

END