Math 25 — Assignment 6

Due Thursday, November 10th, *beginning of class*.

1. Let p be a prime dividing

$$a^5(x-1)^5 - a^4(x-1)^4b + a^3(x-1)^3b^2 - a^2(x-1)^2b^3 + a(x-1)b^4 - b^5$$

for all $x \in \mathbb{Z}$. Prove that $p \mid a$ and $p \mid b$.

Solution: Let $f(x)$ denote the expression from the question. We have in particular that $p \mid f(1) = -b^5$. Because p is prime, we have that $p \mid b$.

Next, $p \mid f(2)$, so in particular p divides

$$a^5(1)^5 - b \cdot (a^4(1)^4 + a^3(1)^3b^1 - a^2(1)^2b^2 + a(1)b^3 - b^4).$$

As $p \mid b$, we have that $p \mid a$.

2. Let a, b be integers such that $\gcd(ab, a+b) = 1$. Prove that a, b are coprime.

Solution: By Bezout's identity we have that there are integers x, y such that

$$xab + y(a+b) = 1.$$

Thus,

$$a(xb + y) + yb = 1.$$

In particular, $\gcd(a, b) \mid 1$, so a, b are coprime.

3. Let $f(x)$ be a polynomial with integer coefficients and let p, q be primes. If $f(x)$ has at least one root modulo p and modulo q, prove that $f(x)$ has a root modulo pq.

Solution: Let α_p denote a root of f modulo p and let α_q denote a root of f modulo q. By the CRT, we can choose $\alpha \in \mathbb{Z}/pq\mathbb{Z}$ such that

$$\begin{aligned} \alpha &\equiv \alpha_p \pmod{p} \\ \alpha &\equiv \alpha_q \pmod{q} \end{aligned}$$

We now claim that $f(\alpha) \equiv 0 \pmod{pq}$. Indeed, write

$$f(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0.$$

Then

$$\begin{aligned} f(\alpha) &\equiv a_n\alpha^n + \cdots + a_1\alpha + a_0 \pmod{p} \\ &\equiv a_n(\alpha \text{ mod } p)^n + \cdots + a_1(\alpha \text{ mod }_p) + a_0 \pmod{p} \\ &\equiv a_n(\alpha_p)^n + \cdots + a_1(\alpha_p) + a_0 \pmod{p} \\ &\equiv f(\alpha_p) \pmod{p} \\ &\equiv 0 \pmod{p} \end{aligned}$$

Similarly $f(\alpha) \equiv 0 \pmod{q}$. But then

$$f(\alpha) \equiv 0 \pmod{p}$$
$$f(\alpha) \equiv 0 \pmod{q}$$

so by the CRT, $f(\alpha) \equiv 0 \pmod{pq}$ (because solutions mod pq are unique; in fact, the CRT lift is an isomorphism). Thus, we have found a root of f modulo pq.

4. Let p be a prime and let $f(x) = x^p \pmod{p}$. Prove that

   (a) $f(0) = 0$ and $f(1) = 1$.

   (b) $f(x + y) \equiv f(x) + f(y) \pmod{p}$.

   (c) $f(xy) \equiv f(x)f(y) \pmod{p}$.

   (d) $f(x)$ is a bijection.

   The map $f(x)$ is called the *Frobenius automorphism*.

   Solution: By Fermat's little Theorem, we have that $x^p \equiv x \pmod{p}$ for all $x \in \mathbb{Z}/p\mathbb{Z}$. Thus,

$$f(x) \equiv x \pmod{p}.$$

   All four parts of this question trivially follow from this observation.

   OK, so let's actually do something more interesting.

   Theorem. *Let R be any finite commutative ring with unity such that $p \equiv 0$ in R. Furthermore, assume that R has no nontrivial nilpotent elements – elements $x \neq 0$ such that $x^m = 0$ for some $m \geq 1$. Then the Frobenius map $f(x) = x^p$ is an automorphism.*

   An example of such a ring is $\mathbb{F}_p[x]/(x^2+1)\mathbb{F}_p[x]$ when p is an odd prime, which has p^2 elements. A non-example of such a ring is $\mathbb{F}_2[x]/(x^2+1)\mathbb{F}_2[x]$, because $x + 1$ is nilpotent.

   Proof. Clearly $f(0) = 0$ and $f(1) = 1$. Let $x, y \in R$. By the Binomial Theorem

$$(x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i.$$

   Because $p \mid \binom{p}{i}$ for all $1 \leq i \leq p$, and p is equivalent to 0 in R, we see that

$$(x + y)^p \equiv x^p + y^p.$$

   Next, $(xy)^p = x^p y^p$ by exponent rules (and the fact that R is commutative).

   The last thing to show is that $f(x)$ is a bijection. We first check that it is injective. If $f(x) = f(y)$, then $x^p - y^p = (x - y)^p = 0$. We must have $x - y = 0$, since R was assumed to have no nilpotent elements. In other words, $x = y$ and $f(x)$ is injective. Because R is finite, we must have that $f\colon R \to R$ is surjective as well. $\square$

5. You'll probably want to open up Sage or Python for this exercise. Let $n := 1333189866793$.

   (a) Compute $a^{n-1} \mod n$ for some example a's. What do you notice? (Hint: use `pow(a,e,n)`)

   (b) Compute the Jacobi symbol $\left(\dfrac{5}{n}\right)$ *by hand*.

   (c) Compute the expression $5^{\frac{n-1}{2}} \pmod{n}$.

(d) Use parts (b) and (c) to prove that n is not prime.

Remark: This type of calculation is the basis for the Solovay-Strassen primality test. It is *much* faster than factoring.

Solution:

(a) It tends to be the case that $a^{n-1} \equiv 1 \pmod{n}$.
Remark: It turns out n is a Carmichael number, so $a^{n-1} \equiv 1 \pmod{n}$ whenever $\gcd(a, n) = 1$.

(b) Using reciprocity we see

$$\left(\frac{5}{n}\right) = (-1)^{\frac{5-1}{2} \cdot \frac{n-1}{2}} \left(\frac{n}{5}\right) = (-1)^{2 \cdot (\text{some integer})} \left(\frac{n \bmod 5}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

(c) We use Sage/Python to check that

```
pow(5, (n-1) // 2, n) == 1
```

(d) If $n > 2$ is prime, then we must have by Euler's criterion

$$5^{\frac{n-1}{2}} \equiv \left(\frac{5}{n}\right) \pmod{n}.$$

However, parts (b) and (c) show that this equivalence does not hold for our particular n. Thus n cannot be prime.

6. Let p, q be odd primes. Prove that

$$\frac{\left(\prod_{i=1}^{p-1} i\right)\left(\prod_{i=1}^{p-1} p+i\right)\cdots\left(\prod_{i=1}^{p-1} \left(\frac{q-1}{2}-1\right)p+i\right)\left(\prod_{i=1}^{\frac{p-1}{2}} \frac{q-1}{2}p+i\right)}{q \cdot 2q \cdot \ldots \cdot \frac{p-1}{2}q} \equiv (-1)^s \left(\frac{q}{p}\right) \pmod{p}$$

where $s = 0$ if $q \equiv 1 \pmod{4}$ and $s = 1$ if $q \equiv 3 \pmod{4}$.

Solution: First, we note that the denominator is non-zero modulo p, and therefore invertible. This follows from the fact that

$$\gcd(q, p) = 1 \quad \gcd\left(\left(\frac{p-1}{2}\right)!, p\right) = 1.$$

The p's in the numerator reduce to 0 modulo p, so we have that the expression under consideration is

$$\equiv \frac{\left(\prod_{i=1}^{p-1} i\right)\left(\prod_{i=1}^{p-1} i\right)\cdots\left(\prod_{i=1}^{p-1} i\right)\left(\prod_{i=1}^{\frac{p-1}{2}} i\right)}{q \cdot 2q \cdot \ldots \cdot \frac{p-1}{2}q} \pmod{p}$$

$$\equiv \frac{\left(\prod_{i=1}^{p-1} i\right)^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)!}{\left(\frac{p-1}{2}\right)! \cdot q^{\frac{p-1}{2}}}$$

$$\equiv \frac{((p-1)!)^{\frac{q-1}{2}}}{q^{\frac{p-1}{2}}}$$

By Wilson's Theorem and Euler's criterion, we have

$$\equiv \frac{(-1)^{\frac{q-1}{2}}}{\left(\frac{q}{p}\right)} \equiv (-1)^{\frac{q-1}{2}} \cdot \left(\frac{q}{p}\right) \pmod{p}.$$

Observe that $\frac{q-1}{2}$ is even if and only if $q \equiv 1 \pmod{4}$. Thus the value of s is as desired.