Solutions to Homework Assignment 3
CS 6104: Algorithmic Number Theory

Problem 1. [Solution Courtesy of Duxing Cai] Chapter 5, Problem 24. Do not look up the answer. Think about the Chinese Remainder Theorem.

Also, derive all solutions for $n = 30$.

Solution:

Let $n = m_1 m_2 ... m_k$, where $m_i, 1 \leq i \leq k$ are powers of distinct primes. We know:

$$x^2 \equiv x \pmod{n} \Longleftrightarrow x(x-1) \equiv 0 \pmod{n}.$$

Note that, m_i are relatively prime, we have:

$$\{x \mid x(x-1) \equiv 0 \pmod{n = m_1 m_2 ... m_k}\} \Longleftrightarrow \{x \mid x(x-1) \equiv 0 \pmod{m_i}), \forall 1 \leq i \leq k\}$$

i.e. The solutions of $x(x-1) \equiv 0 \pmod{n}$ are equivalent to the solutions of the systems:

$$x(x-1) \equiv 0 \pmod{m_i}, \forall 1 \leq i \leq k$$

So the numbers of solutions should be the same. Also note that:

$$gcd(x, x-1) = 1.$$

So the solution of $x(x-1) \equiv 0 \pmod{m_i}$ must satisfy:

$$x \equiv 0 \text{ or}$$
$$x - 1 \equiv 0 \Rightarrow x \equiv 1 \pmod{m_i}, \forall 1 \leq i \leq k.$$

i.e. For each m_i we have two choices. So we can get 2^k different systems:

$$x \equiv e_i, \quad \pmod{m_i}, \forall 1 \leq i \leq k,$$

where $e_i = 0$ or 1.

By the Chinese Remainder Theorem, each system must have one unique solution modulo $n = m_1 m_2 ... m_k$. Furthermore, by the Extended Chinese Remainder Theorem we know these systems have distinct solutions. Actually, if two different system have the same solution x, then within these two system must exist the following two different equations associated with some m_i:

$$x \equiv 0 \pmod{m_i}$$

$$x \equiv 1 \pmod{m_i}$$

But this is impossible.

So we can conclude that the equation $x^2 \equiv x \pmod{n}$ has exactly 2^k different solutions. Now we can derive all solutions for $n = 30$:

Since $n = 30 = 2 * 3 * 5$, we can get the following $2^3 = 8$ systems:

- $x \equiv 0 \pmod 2, x \equiv 0 \pmod 3, x \equiv 0 \pmod 5$
- $x \equiv 1 \pmod 2, x \equiv 0 \pmod 3, x \equiv 0 \pmod 5$
- $x \equiv 0 \pmod 2, x \equiv 1 \pmod 3, x \equiv 0 \pmod 5$
- $x \equiv 1 \pmod 2, x \equiv 1 \pmod 3, x \equiv 0 \pmod 5$
- $x \equiv 0 \pmod 2, x \equiv 0 \pmod 3, x \equiv 1 \pmod 5$
- $x \equiv 1 \pmod 2, x \equiv 0 \pmod 3, x \equiv 1 \pmod 5$
- $x \equiv 0 \pmod 2, x \equiv 1 \pmod 3, x \equiv 1 \pmod 5$
- $x \equiv 1 \pmod 2, x \equiv 1 \pmod 3, x \equiv 1 \pmod 5$

With the Extended Chinese Remainder Theorem, system (1) can be reduced to the following system:

$$x = 2 * t \equiv 0 \pmod 3$$
$$x \equiv 0 \pmod 5$$

Since $x = 2 * t \equiv 0, \pmod 3 \Longleftrightarrow t \equiv 0 \pmod 3$, we get: $t = 3 * h$ for some h. So the system becomes: $x = 6 * h \equiv 0 \pmod 5$. Thus the solution of this system is:

$$x_1 \equiv 0 \pmod{30}$$

Similarly we can find all the other solutions as following:

$$\begin{gathered} x_2 \equiv 15 \pmod{30} \\ x_3 \equiv 10 \pmod{30} \\ x_4 \equiv 25 \pmod{30} \\ x_5 \equiv 6 \pmod{30} \\ x_6 \equiv 21 \pmod{30} \\ x_7 \equiv 16 \pmod{30} \\ x_8 \equiv 1 \pmod{30} \end{gathered}$$

Problem 2. [Solution Courtesy of Cara Struble] Use Theorem 5.8.1 to compute the Legendre symbol

$$\left(\frac{958816}{129527}\right)$$

is two distinct ways. If

$$\left(\frac{958816}{129527}\right) = 1,$$

then find a solution x to the congruence

$$x^2 \equiv 958816 \pmod{129527}.$$

(Consult Theorem 7.1.1 and Corollary 7.1.2.)

Using Theorem 5.8.1, there are many different ways to compute a Legendre symbol. The first method I present is simple and direct. Using rule (1), we have

$$\left(\frac{958816}{129527}\right) \equiv 958816^{(129527-1)/2}\ (\mathrm{mod} 129527)$$

Mathematica computes the right hand side of the equivalence to be 1, so the Legendre symbol is 1.

Another way to compute the Legendre symbol is to break up 958816 using rule (2). The number 958816 has prime factorization $2^5 \cdot 19^2 \cdot 83$. So

$$\left(\frac{958816}{129527}\right) = \left(\frac{2^5}{129527}\right)\left(\frac{19^2}{129527}\right)\left(\frac{83}{129527}\right)$$

Now we can look at each of these individually. Using rule (5),

$$\begin{aligned}\left(\frac{2}{129527}\right) &= (-1)^{\frac{129527^2-1}{8}} \\ &= 1.\end{aligned}$$

So

$$\left(\frac{2^5}{129527}\right) = 1.$$

Since 129527 does not divide 19, we can apply rule (4) and get

$$\left(\frac{19^2}{129527}\right) = 1.$$

Since 83 is prime, rule (6) can be used to flip the numbers and the sign is determined by raising -1 to $(\frac{83-1}{2} \cdot \frac{129527-1}{2})$. This power comes out odd so we have

$$\left(\frac{83}{129527}\right) = -\left(\frac{129527}{83}\right).$$

Next we apply rule (3), choosing $b = 47$ so that $129527 \equiv 47(\mathrm{mod}\ 83)$. And we get

$$-\left(\frac{129527}{83}\right) = -\left(\frac{47}{83}\right).$$

Using rule (6), we once again get -1 to an odd power, so

$$-\left(\frac{47}{83}\right) = \left(\frac{83}{47}\right).$$

Now rule (3) applies again if we choose $b = 36$ because $83 \equiv 36 (\bmod 47)$. So

$$\left(\frac{83}{47}\right) \;=\; \left(\frac{36}{47}\right).$$

Since 36 is 6^2 and 47 does not divide 6, we can apply rule (4) and get that

$$\begin{aligned} \left(\frac{83}{129527}\right) &= \left(\frac{6^2}{47}\right) \\ &= 1. \end{aligned}$$

Thus,

$$\begin{aligned} \left(\frac{958816}{129527}\right) &= \left(\frac{2^5}{129527}\right)\left(\frac{19^2}{129527}\right)\left(\frac{83}{129527}\right) \\ &= 1 \cdot 1 \cdot 1 \\ &= 1. \end{aligned}$$

The second part of the problem is to solve

$$x^2 \;\equiv\; 958816 \pmod{129527}$$

which can be simplified to

$$x^2 \;\equiv\; 52127$$

Now Corollary 7.1.2 can be applied to solve for x:

$$\begin{aligned} x &= 52127^{\frac{129527+1}{4}} \pmod{129527} \\ &= 107866. \end{aligned}$$