

**Math 104A, Number Theory, Fall 2002.**  
**Summary of Lecture 14.**

**Generalized CRT:** The system of equations

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ (*) \quad x &\equiv b_r \pmod{m_r}. \end{aligned}$$

has a solution if and only if  $b_i \equiv b_j \pmod{(m_i, m_j)}$  for every  $i$  and  $j$ . We proved this following 3.3.4, and did example 3.3.5.

**Recall the homework problem 2.5 #13.** Show that if  $m$  and  $n$  are relatively prime, then

$$\sum_{k=1}^{n-1} \left\lfloor \frac{mk}{n} \right\rfloor = \frac{(n-1)(m-1)}{2}.$$

A student in the class found a beautiful proof of this. Consider the fractional part of  $mk/n$ ,

$$\frac{mk}{n} - \left\lfloor \frac{mk}{n} \right\rfloor = \frac{r_k}{n}.$$

Here,  $r_k$  is the remainder when  $mk$  is divided by  $n$ , so  $0 \leq r_k < n$  and

$$mk \equiv r_k \pmod{n}.$$

However, we claim that because  $(m, n) = 1$ , the list of numbers  $r_1, r_2, \dots, r_{n-1}$  is just some permutation of the list  $1, 2, \dots, n-1$ . First note that  $r_k \neq 0$ , since

$$n|mk \quad \rightarrow \quad n|k.$$

Furthermore,  $r_k \neq r_j$  for  $j \neq k$ , since then

$$n|m(k-j) \quad \rightarrow \quad n|(k-j),$$

but  $|k-j| < n$ . Hence  $r_1, r_2, \dots, r_{n-1}$  are distinct numbers between 1 and  $n-1$  and so they are some permutation of  $1, 2, \dots, n-1$ . Hence

$$\sum_{k=1}^{n-1} \left( \frac{mk}{n} - \left\lfloor \frac{mk}{n} \right\rfloor \right) = \sum_{k=1}^{n-1} \frac{r_k}{n} = \sum_{k=1}^{n-1} \frac{k}{n}.$$

1

But then

$$\sum_{k=1}^{n-1} \left\lfloor \frac{mk}{n} \right\rfloor = \sum_{k=1}^{n-1} \frac{mk}{n} - \sum_{k=1}^{n-1} \left( \frac{mk}{n} - \left\lfloor \frac{mk}{n} \right\rfloor \right) = (m-1) \sum_{k=1}^{n-1} \frac{k}{n} = \frac{(m-1)(n-1)}{2}.$$

Next time, we will start discussing polynomial congruences. If

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0,$$

we want to solve

$$(**) \quad f(x) \equiv 0 \pmod{m}.$$

We have already solved the case when  $f(x) = ax + b$ . The strategy for general polynomials is to find the prime factorization of  $m$  and solve  $(**)$  when  $m$  is replaced by a prime factor of  $m$ , then use this to solve  $(**)$  when  $m$  is replaced by a prime power, and finally to put these solutions together to solve  $(**)$  for general  $m$ .