Mathematics 4300 – Foundations of Algebra – Fall 1999

8. The Chinese Remainder Theorem. Think of addition of hours on the clock....6 o'clock + 9 hours = 3 o'clock, etc.... this is "addition mod 12". There is a similar addition and also a multiplication with 12 replaced by any natural number m (which we'll call "clock arithmetic"). This arithmetic produces a field with m elements when m is prime. The Chinese remainder theorem is a fundamental theorem about clock arithmetic which gives us some idea about what is going on when m is not a prime.

To get started, we need a slight improvement on division with remainders:

Division of Integers with Remainders: Suppose a is an integer and m is a natural number. Then there is a unique "quotient" integer q and "remainder" integer r such that:

$$a = mq + r \text{ and } \ r \text{ is between } 0 \text{ and } m - 1$$

Proof: If $a \geq m$, we have already proved this. If $a < m$, on the other hand, then $m - a > 0$ so $2m - a > m$, and therefore division with remainders works for $2m - a$. Thus $2m - a = mq' + r'$ for some q' and r'. Then:

$a = m(2 - q')$ if $r' = 0$ so we take $q = 2 - q'$ and otherwise

$a = m(1 - q') + (m - r')$ so we take $q = 1 - q'$ and $r = m - r'$.

Next, we say a is **divisible** by m, written $m|a$, if $a = mq$.

Definition: We say integers a and b are **congruent mod** m, written:

$$a \equiv b \pmod{m}$$

if $a - b$ is divisible by m, which is the same as saying that a and b have the same remainder when divided by m.

The following are clear from the definition:

(i) $a \equiv a \pmod{m}$

(ii) if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$

(iii) if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.

This tells us that congruence mod m is an **equivalence relation**. More practically, it tells us that we can treat congruence as though it were an equation in the sense that we can perform substitutions.

It is useful to picture congruences by putting the integers on the face of a clock. Place 0 at 12 o'clock and divide the circle into m equal parts so that 1 is at (roughly) 1 o'clock up to $m-1$, which is at (roughly) 11 o'clock. We continue by wrapping around in both directions so that m is at 12 o'clock, $m+1$ is at (roughly) 1 o'clock, etc. and -1 is at (roughly) 11 o'clock, etc. We'll call this an m-**clock** (so that the ordinary clock is a 12-**clock**).

Then $a \equiv b \pmod{m}$ if a and b locate the same point on the m-clock.

Note: When we think of it this way, congruence mod m is analogous to equality for rational numbers. Just as we located fractions as points on the number-line, we are locating integers as points on a "number"-clock. The difference is that here there is not just one such clock, but a different one for each integer m. That is, of course, why m is built into the notation.

Arithmetic on the number-clock:

Addition. Suppose r and s are points on the m-clock. Then we define $r+s$ by finding integers a and b which locate r and s, and locating their sum on the m-clock. We need to check that this is well-defined (just as we needed to check that the formula for multiplication of rational numbers was well-defined). That is, we need to check that if:

$$a \equiv a' \pmod{m} \quad \text{and} \quad b \equiv b' \pmod{m}$$

(so that a and a' locate the **same** point and similarly for b and b') then:

$$a + a' \equiv b + b' \pmod{m}.$$

So let's check it. We have: $a - a' = mq$ and $b - b' = mq'$ so that $(a+b)-(a'+b') = (a-a')+(b-b') = m(q+q')$, which indeed implies $a + b \equiv a' + b' \pmod{m}$. Check!

The properties (a)-(d) for addition are now easy to verify.

(a) Clock addition is associative. This is because ordinary addition of integers is associative.

$$(a+b)+c \equiv a+(b+c) \pmod{m} \text{ because } (a+b)+c = a+(b+c)$$

(b) 12 o'clock is the additive identity. 0 represents 12 o'clock, and

$$0 + a \equiv a \pmod{m} \text{ because } 0 + a = a$$

(c) Additive inverses always exist.

$$a + (-a) \equiv 0 \pmod{m} \text{ because } a + (-a) = 0$$

So we can do clock subtraction. Notice that the point represented by $-n$ is obtained by moving n steps **counterclockwise** from 12 o'clock, so on the ordinary 12-clock, 11 o'clock is the additive inverse to 1 o'clock, 10 o'clock is the additive inverse to 2 o'clock, etc.

(d) Clock addition is commutative. This is because ordinary addition of integers is commutative.

$$a + b \equiv b + a \pmod{m} \text{ because } a + b = b + a$$

Multiplication. Suppose r and s are points on the m-clock. Then we define $r \cdot s$ by representing r and s by integers a and b and locating $a \cdot b$ on the m-clock. In this case, we need to show that if $a - a'$ and $b - b'$ are both divisible by m, then $ab - a'b'$ is divisible by m so that ab and $a'b'$ locate the same point on the m-clock. This is only slightly harder than addition. If we write: $a - a' = mq$ and $b - b' = mq'$, then

$$ab - a'b' = a(b - b') + (a - a')b' = a(mq') + (mq)b' = m(aq' + qd)$$

so that indeed $ab \equiv a'b' \pmod{m}$.

Once again, we easily get some of the properties for multiplication:

(e) Clock multiplication is associative. This is again because ordinary multiplication of integers is associative.

$$(ab)c \equiv a(bc) \pmod{m} \text{ because } (ab)c = a(bc)$$

(f) Clock multiplication distributes with clock addition. Again,

$$a(b + c) \equiv ab + ac \pmod{m} \text{ because } a(b + c) = ab + ac$$

(g) 1 locates the multiplicative identity on the m-clock. Again,

$$1 \cdot a \equiv a \pmod{m} \text{ because } 1 \cdot a = a$$

(i) Clock multiplication is commutative. Again,

$$ab \equiv ba \pmod{m} \text{ because } ab = ba$$

This only leaves multiplicative inverses. Recall that only 1 and -1 had integer multiplicative inverses. This makes the following rather surprising.

Proposition 4: The point located by n on the m-clock has a multiplicative inverse exactly when $\gcd(m, n) = 1$.

Proof: Suppose that $\gcd(m, n) = 1$. Then by Proposition 3, we know that we can write:

$$1 = am + bn$$

for some integers a and b. But then m divides $bn - 1$ so $bn \equiv 1 \pmod{m}$ which tells us that b locates the multiplicative inverse! On the other hand, if there is a multiplicative inverse, suppose b locates it. Then m divides $bn - 1$ by Proposition 3, and it follows that $\gcd(m, n) = 1$.

Corollary: The m-clock is a field exactly when m is a prime number.

Proof: We've seen that if p is a prime number, $\gcd(p, n) = 1$ whenever p does not divide n. This means that **every** point on the p-clock except 12 o'clock (which is the additive identity) has a multiplicative inverse, so it satisfies property (h) and is thus a field. If m is not a prime, then write $m = kl$ for smaller k and l, and neither of the points located by k and l are at 12 o'clock (because k and l are between 1 and $m - 1$). But k does not have a multiplicative inverse. If it did, say if $bk \equiv 1 \pmod{m}$, then we'd have $0 \equiv bkl \equiv l \pmod{m}$. But l is not at 12 o'clock, as we've already noted.

Example: The ordinary 12-clock.

1 o'clock is the multiplicative identity.

$5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$, so $5, 7, 11$ are their own inverses, and

$2, 3, 6, 8, 9, 10$ do not have multiplicative inverses.

So we've found a bunch more fields! In fact, for every prime number p, we now have the p-clock, which is a field with p elements. We'll denote this field by $\mathbf{F}_p$. Everything we need to know about $\mathbf{F}_p$ is contained in the addition and multiplication tables, where we carry out the addition or multiplication, and then take remainders mod p:

The field $\mathbf{F}_2$...or arithmetic mod 2:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

The field $\mathbf{F}_3$...or arithmetic mod 3:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Finite fields suggest some interesting new questions. Here's a familiar one from the complex numbers. When can we solve $x^n = 1$ in arithmetic mod p?

Fermat's (Little) Theorem: If p is a prime and a is an integer, then

$$a^p \equiv a \pmod{p}$$

Proof: This is clearly true for $a = 0$. Let's first prove it for all natural numbers by induction.

(a) $P(1)$. $1^p = 1 \equiv 1 \pmod{p}$. Obviously.

(b) Suppose it is true for $a = n$. Then using the binomial theorem:

$$(n+1)^p = n^p + pn^{p-1} + ... + \binom{p}{m} n^m + ... + pn + 1.$$

But p divides $\binom{p}{m}$ whenever m is different from 0 and m (homework!), so p divides $(n+1)^p - n^p - 1$ and we therefore get:

$$(n+1)^p \equiv n^p + 1 \pmod{p}$$

Since $n^p \equiv n \pmod{p}$ by our assumption, we get:

$$(n+1)^p \equiv n + 1 \pmod{p}$$

by substituting, which is what we needed to prove.

Finally, we prove the little theorem when $a = -n$. In that case:

$$a^p = (-n)^p = (-1)^p n^p \equiv (-1)^p n = (-1)^{p-1} a \pmod{p}$$

Now either p is odd, in which case $(-1)^{p-1} = 1$, and we get the theorem, or else $p = 2$, and since $-1 \equiv 1 \pmod{2}$, we get the theorem here, too!

Corollary: Everything in $\mathbf{F}_p$ except 0 is a $(p-1)$st root of 1.

Proof: Fermat's little theorem tells us that $s^p = s$ for any $s \in \mathbf{F}_p$. If $s \neq 0$, then s has a multiplicative inverse, so we can multiply both sides of this equation by s^{-1} to get $s^{p-1} = 1$, showing that s is a $(p-1)$st root of 1.

Of course, a square root of 1 is also a fourth root, etc. If we are given s, then it is natural to ask about the **smallest** positive n so that $s^n = 1$.

Corollary: In $\mathbf{F}_p$, the smallest positive n so that $s^n = 1$ always divides $p-1$.

Proof: Suppose $s^n = 1$ and $n < p-1$. Then $p - 1 = nq + r$ with $r < n$. Raising s to both sides gives

$$1 = s^{p-1} = s^{nq+r} = s^{nq}s^r = (s^n)^q s^r = s^r$$

so that $s^r = 1$. Thus if n is **smallest**, then $r = 0$, and n divides $p-1$.

Example: When $p = 17$, we examine powers of 2:

$$2, 4, 8, 16, 32 \equiv 15 \pmod{17}, 30 \equiv 13, 26 \equiv 9, 18 \equiv 1$$

so that $2^8 = 1$ in $\mathbf{F}_{17}$, 8 is the smallest power, and indeed 8 divides 16.

Application to repeating decimals: We wondered earlier about how long it takes for the decimal expansion of $\frac{1}{n}$ to repeat. We are now in a position to give a partial answer when $n = p$ is a prime.

Claim: If $p \neq 2, 5$ and the decimal expansion of $\frac{1}{p}$ repeats for the first time after n steps, then n divides $p-1$.

Proof: Consider the sequence represented by $10, 10^2, 10^3, \ldots$ in $\mathbf{F}_p$. By our assumption on p, we know 10 represents something nonzero in $\mathbf{F}_p$, so by the corollary above, we have that $n|p-1$ the first time $10^n = 1$ in $\mathbf{F}_p$. But this tells us that p divides $10^n - 1$, and we can write $pm = 10^n - 1$ or:

$$\frac{1}{p} = \frac{m}{10^n - 1}$$

which tells us that the decimal expansion of $\frac{1}{p}$ is just m times the decimal expansion $0.\overline{0000....1}$ ($n-1$ zeroes followed by a 1). This clearly consists of the digits of m repeating every n steps...and n divides $p-1$.

Example: $\frac{1}{11} = 0.\overline{09}$ repeats after two steps, and $10^2 = 100 \equiv 1 \pmod{11}$. In case $p = 17$, we don't get $10^n \equiv 1$ until $n = 16$ (the last possible!).

Finally, suppose we are given natural numbers m and n and integers $0 \le s < m-1$ and $0 \le t < n-1$. We can think of s and t as elements of the m-clock and n-clock (and we do not assume m and n are primes). We ask: Is there an integer which represents **both** s and t simultaneously? In mathematical notation, we are asking for a solution to the two congruences:

$$x \equiv s \pmod{m} \quad \text{and} \quad x \equiv t \pmod{n}$$

Such a simultaneous solution need not exist if $\gcd(m,n) \ne 1$. However:

The Chinese Remainder Theorem: If $\gcd(m,n) = 1$, write $1 = am + bn$. Then we get a solution to the two congruences above by setting:

$$x = amt + bns.$$

Proof: From the equation $1 = am + bn$, we notice that:

$$bn \equiv 1 \pmod{m} \quad \text{and} \quad am \equiv 1 \pmod{n}.$$

Our choice for x give us: $x \equiv bns \pmod{m}$ and $x \equiv amt \pmod{n}$

From the first congruences we get $bns \equiv b \pmod{m}$ and $amt \equiv a \pmod{n}$, which we may substitute into the second congruences to prove the theorem.

This solution x may be large, or negative, but:

Improvement: There is exactly one solution between 0 and $mn-1$.

Proof: Start with the solution coming from the theorem and divide it by mn with remainders. Then $x = (mn)q + r$ and $x \equiv r \pmod{m}$ and $x \equiv r \pmod{n}$ so r solves the two congruences and is between 0 and $mn-1$.

Suppose s was another solution between 0 and $mn-1$, and suppose that $r > s$. Then $m|(r-s)$ and $n|(r-s)$, so $\operatorname{lcm}(m,n) \le r-s$. But $\operatorname{lcm}(m,n) = mn$ because $\gcd(m,n) = 1$ (Homework!). But $r-s$ cannot be this big because $r < mn$. We conclude that and there is no such s. Similarly, there is no other solution between 0 and $mn-1$ larger than r either. So r is the only solution between 0 and $mn-1$.

Exercises:

1. (a) Fill in the addition and multiplication tables for $\mathbf{F}_5, \mathbf{F}_7, \mathbf{F}_{11}$ and $\mathbf{F}_{13}$.

(b) For every element $r \neq 0, 1$ of every field above, write out the sequence:

$$r, r^2, r^3, \ldots$$

stopping when you first hit 1.

Notice that in each of these cases, there are elements which require the full $p-1$ steps before you hit 1. Notice also that if r is such an element, then $r, r^2, \ldots, r^{p-1}$ are **all** of the elements of $\mathbf{F}_p - \{0\}$.

(c) Notice that there are four square roots of 1 on the 12-clock. Prove that there are only two square roots of 1 on a p-clock when p is prime.

2. The Chinese Remainder Theorem gives a constructive method for solving the congruences $x \equiv r \pmod{m}$ and $x \equiv s \pmod{n}$ for x between 0 and $mn - 1$. That is, first you solve: $1 = am + bn$, then you divide by mn and take remainders. Use this method to solve the following problem:

"Everyone in my family is less than 99 years old. When you divide their ages by 9 and 11, you get the following remainders:"

(a) Me. 1 (mod 9) and 4 (mod 11).

(b) Mom. 5 (mod 9) and 4 (mod 11).

(c) Dad. 6 (mod 9) and 5 (mod 11).

(d) Grandpa. 3 (mod 9) and 5 (mod 11).

(e) Sophie. 6 (mod 9) and 6 (mod 11).

How old is everyone?