Math 8: Prime Factorization and Congruence

Spring 2011; Helena McGahagan

Prime Factorization

The main result in Chapter 11 is the Fundamental Theorem of Arithmetic: This is the statement that every integer $n \geq 2$ has a *unique* prime factorization. Of course, to make this statement true, we have to require that the prime factorization of a number lists the primes in order: that is, the prime factorization of 20 is $2 \cdot 2 \cdot 5$ and *not* $2 \cdot 5 \cdot 2$ or $5 \cdot 2 \cdot 2$. We can now state this theorem precisely:

The Fundamental Theorem of Arithmetic (Theorem 11.1)
Let n be an integer with $n \geq 2$. Then, there are unique prime numbers satisfying $p_1 \leq p_2 \leq ... \leq p_k$ such that $n = p_1 \cdot p_2 \cdot ... \cdot p_k$.

Note: We have already shown in lecture that every integer $n \geq 2$ has a prime factorization. To show uniqueness, simply assume there are two sets of prime numbers: $p_1 \leq ... \leq p_k$ and $q_1 \leq ... \leq q_l$ such that $n = p_1...p_k = q_1...q_l$; then, prove that $k = l$ and $p_i = q_i$ for all $1 \leq i \leq k$.

There are several consequences of the Fundamental Theorem of Arithmetic. Review the statements and proofs of Propositions 11.1, 11.2, and 11.4 in the book, and notice that many of the proofs follow by writing down prime factorizations for all the numbers involved and using uniqueness to match up the terms on each side. One of these useful consequences (Prop. 11.2(iii)), is the fact that (for $a, b \geq 1$) $\text{lcm}(a, b) = ab/\text{hcf}(a, b)$. (*Recall that we were also able to prove this without using prime factorization! See Exercise #4.*)

A **Diophantine equation** is an equation for which the solutions are required to be integers. For instance, in Chapter 10, we learned that *linear* Diophantine equations of the form $d = sa + tb$ can be solved if $d = \text{hcf}(a, b)$ (or even if $\text{hcf}(a, b) \mid d$). Once we have a solution of this equation, we have infinitely many. In fact, we proved the following theorem in class about the general form of the solution:

THEOREM Let $a, b \in \mathbb{Z}$ and let $d = \text{hcf}(a, b)$. Since $d \mid a$ and $d \mid b$, there exist $a', b' \in \mathbb{Z}$ such that $a = a'd$ and $b = b'd$. Assume that we know one solution (s_o, t_o) to the linear Diophantine equation $d = sa + tb$. Then, every solution of the equation $d = sa + tb$ is of the form

$$s = s_o + nb' \quad \text{and} \quad t = t_o - na' \quad \text{for } n \in \mathbb{Z}.$$

Proof: First, we note that a' and b' are coprime (*prove this!*) The following simple computation shows that, given any n, $s = s_o + nb'$ and $t = t_o - na'$ is a solution of the Diophantine equation:

$$(s_o + nb')a + (t_o - na')b = (s_o a + t_o b) + n(b'a - a'b) = d + n(b'a'd - a'b'd) = d.$$

On the other hand, assume we are given a solution $s, t \in \mathbb{Z}$ of the equation $d = sa + tb$. We need to prove that there exists an $n \in \mathbb{Z}$ such that s and t are of the form given above. Since we have both $d = s_o a + t_o b$ and $d = sa + tb$, we subtract:

$$0 = (s_o - s)a + (t_o - t)b = ((s_o - s)a' - (t - t_o)b')d.$$

Since we know that $d \geq 1$, this means that $(\star)$ $a'(s_o - s) = (t - t_o)b'$. Therefore, we know that $b' \mid a'(s - s_o)$. Since b' and a' are coprime, we must have $b' \mid (s - s_o)$. In other words, there exists an $n \in \mathbb{Z}$ such that $s = s_o + nb'$. We can plug this into the equation $(\star)$ and solve for t: $t = t_o - na'$. Therefore, the solution s and t is of the form given above. $\square$

Example How many ways can you pay for an item worth \$2.65 using only quarters and dimes? Use the general form of the solution to the equation $10s + 25t = 265$ to prove there are 5 positive solutions. (*You should find that* (s, t) *is* $(4, 9), (9, 7), (14, 5), (19, 3),$ *or* $(24, 1)$.)

Of course, it's much harder to determine if non-linear equations have solutions or not! As an example from your book (pg. 95), Proposition 11.4 (the fact that if a product ab is an n^{th} power, then each of a and b must be an n^{th} power) is useful in proving that $4x^2 = y^3 + 1$ has a unique solution (namely, $x = 0$ and $y = -1$). By the way, can you think some examples for Proposition 11.4? That is, think of integers a and b such that ab is a perfect square (or perfect cube, etc).

Congruence

Definitions Let $m \in \mathbb{N}$.

- For any $a, b \in \mathbb{Z}$, we say "a is **congruent** to b modulo m" if $m \mid (b - a)$. In symbols, we write this as $a \equiv b \mod m$.
- We can use congruence to define a system $\mathbb{Z}_m$ called "**the integers modulo** m." $\mathbb{Z}_m$ is defined to be a set with m elements: $\{[0], [1], [2], ..., [m-1]\}$. We also define the operations $+$ and $\times$ on the elements of this set: For any $[x], [y] \in \mathbb{Z}_m$, find the usual sum $x+y$. This number is congruent to one (and only one) of the numbers $0, 1, ..., m-1$ modulo m (see Proposition 13.1 – note that it follows directly from the definition of modulo m and from the division algorithm), so we find $0 \leq z < m$ such that $x + y \equiv z \mod m$. Then, we define $[x] + [y] = [z]$ in the system $\mathbb{Z}_m$. We do the same thing for multiplication: we define $[x][y] = [w]$ if $xy \equiv w \mod m$.

The symbol "$\equiv \mod m$" acts a lot like a regular equal sign: See Proposition 13.2. For instance, we can add and multiply the same thing on both sides: See Proposition 13.3 (and 13.4, which follows by just repeatedly applying Proposition 13.3). This means we can perform arithmetic on congruence equations: For example, once we know $6 \equiv 36 \mod 10$ and $7 \equiv -3 \mod 10$, we can add these two equations to find that $13 \equiv 33 \mod 10$, or multiply them to find that $42 \equiv -108 \mod 10$. The one thing we have to be careful about is that we can't necessarily divide! Even though $6 \equiv 36 \mod 10$ and $6 \equiv 6 \mod 10$, it is not true that $6/6 = 1$ will be equal to $36/6 = 6$ modulo 10. However, we can divide in the following special case:

PROPOSITION 13.5
(1) Let a and m be coprime integers. If $x, y \in \mathbb{Z}$ are such that $xa \equiv ya \mod m$, then $x \equiv y \mod m$.

(2) Let p be a prime number, and let $a \in \mathbb{Z}$ be such that $p \nmid a$. If $x, y \in \mathbb{Z}$ are such that $xa \equiv ya \mod m$, then $x \equiv y \mod m$.

In other words, we can divide an equation on both sides as long as we divide by something coprime to the number m. The proof follows from a theorem we already know about division and coprime numbers (see the book for a detailed proof.) Similarly, the next proposition follows from the definition of congruence modulo m and our previous theorems about when $d = sa + tb$ has solutions:

PROPOSITION 13.6
Let $m \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. The congruence equation $ax \equiv b \mod m$ has a solution $x \in \mathbb{Z}$ if and only if $\text{hcf}(a, m) \mid b$.

Proof: Let $d = \text{hcf}(a, m)$.
We first prove the ($\Rightarrow$) direction. Assume that there exists $x \in \mathbb{Z}$ such that $ax \equiv b \mod m$. Then, by the definition of congruence, $m \mid (b - ax)$. In other words, there exists $q \in \mathbb{Z}$ such that $b - ax = qm$. Since $d \mid a$ and $d \mid m$, it follows that $d \mid (ax + qm)$; i.e., $\text{hcf}(a, m) \mid b$.
We now prove the ($\Leftarrow$) direction. Assume that $d \mid b$. Therefore, $d = kb$ for some $k \in \mathbb{Z}$. Since $d = \text{hcf}(a, m)$, we know that there exist integers $s, t \in \mathbb{Z}$ such that $d = sa + tm$. Then, $b = kd = (ks)a + (kt)m$. We see from this equation that $(ks)a \equiv b \mod m$. Therefore, we have found a solution $x = ks$ of the congruence equation. $\square$

Fermat's Little Theorem
Let p be a prime number and let $a \in \mathbb{Z}$ be such that $p \nmid a$. Then $a^{p-1} \equiv 1 \mod p$.

This tells us that many equivalence relations (that would otherwise take a lot of arithmetic to check) are true! For instance, it must be true that $303^{96} \equiv 1 \mod 97$. There are several simple consequences of Fermat's Little Theorem:

COROLLARY 1 Let p be a prime number and let a be any integer. Then $a^p \equiv a \mod p$

Proof: There are two cases: either $p \mid a$ or $p \nmid a$. In the case $p \mid a$, then clearly $a^p \equiv a \equiv 0 \mod p$. In the case $p \nmid a$, Fermat's Little Theorem applies and we know that $a^{p-1} \equiv 1 \mod p$. Multiplying both sides of this equation by a yields $a^p \equiv a \mod p$. □

COROLLARY 2 Let p be a prime number. If $[a]$ is any non-zero number in $\mathbb{Z}_p$, then there exists a number $[b]$ in $\mathbb{Z}_p$ such that $[a][b] = 1$. (In other words, there exists an *inverse* of the number $[a]$ in $\mathbb{Z}_p$!)

Proof: If $[a] \neq [0]$, then we know $0 < a < p$. Therefore, $p \nmid a$. Find $0 \leq b < p$ such that $b \equiv a^{p-2} \mod m$. From Fermat's Little Theorem, we know that $[a][b] = [1]$ (since $ab \equiv a \cdot a^{p-2} \equiv a^{p-1} \equiv 1 \mod p$). □

PROPOSITION 14.1 Let p and q be distinct prime numbers. Let $a \in \mathbb{Z}$ be such that $p \nmid a$ and $q \nmid a$. Then, $a^{(p-1)(q-1)} \equiv 1 \mod (pq)$.

See the book for the proof, which follows from using Fermat's theorem twice to find that $a^{(p-1)(q-1)}$ is congruent to 1 both modulo p and modulo q. Fermat's theorem also gives us a method that we can sometime use to test that a large number is *not* prime:

Fermat's Test for Primes Fix $p, a \in \mathbb{Z}$ with $0 < a < p$. If $a^{p-1} \not\equiv 1 \mod p$, then p is not prime.

Proof: Fermat's theorem tells us that the statement "if p is prime, then $a^{p-1} \equiv 1 \mod p$" is true; this theorem is the contrapositive. □

Finally, Fermat's theorem gives us a procedure for calculating k^{th} roots modulo m.

PROPOSITION 14.2
Let p be a prime number, and let $k \in \mathbb{N}$ be coprime to $p-1$. Then,
(i) There exists $s \in \mathbb{N}$ such that $sk \equiv 1 \mod (p-1)$
(ii) For any $b \in \mathbb{Z}$ such that $p \nmid b$, $x^k \equiv b \mod p$ has a unique solution satisfying $0 < x < p$.
In particular, we know that the solution $x \equiv b^s \mod p$.

The proof of this proposition tells us exactly what to do to find the solution x: First, find *positive* integers s and t that solve the equation $sk - t(p-1) = 1$. (We can do this since k and $p-1$ are coprime and both positive.) Clearly s satisfies $sk \equiv 1 \mod (p-1)$. Then, simply show that $b^s \mod p$ is the only possible solution of $x^k \equiv b \mod p$:

It is *a* solution since $(b^s)^k \equiv b^{sk} \equiv b^{1+t(p-1)} \equiv b(b^{p-1})^t \equiv b \mod p$, where the last step follows by the corollary to Fermat's theorem. Moreover, *any* solution x must satisfy $x^{p-1} \equiv 1 \mod p$ (again by Fermat's theorem; notice that since $p \nmid b$, we know that $p \nmid x$.). Show that this implies $x \equiv b^s \mod p$. This proves that $b^s \mod p$ is the *only* solution modulo p.

EXAMPLES These are all examples from lecture. See if you can answer them without looking back at your lecture notes.

1. If today is Tuesday, what day will it be in 3118 days from now?
2. What is the remainder when 2^{37} is divided by 7?
3. What is the remainder when 2^{39} is divided by 13?
4. What is the remainder when $4^{10} \cdot 7^7$ is divided by 5?
5. Show that $43296 \times 1742 - 51436$ cannot be equal to 74907256 by "casting out the nines."
6. Find all solutions to $4x \equiv 2 \mod 6$.
7. Find all solutions to $2x = 1$ in $\mathbb{Z}_4$.
8. Find all solutions to $20x \equiv 8 \mod 44$.
9. Find $[2]^{-1}$ in $\mathbb{Z}_7$.
10. Find $[2]^{-1}$ in $\mathbb{Z}_{31}$.
11. Find all solutions to $x^7 + x^3 + 2x^2 + 4 \equiv 0 \mod 7$.
12. Can you use Fermat's test to determine whether or not 1479 is prime?
13. Can you use Fermat's test to determine whether or not 561 is prime?
14. Solve $x^{25} = 3 \mod 37$.