

UMASS AMHERST MATH 471 FALL 2006, F. HAJIR

QUICK REVIEW FOR EXAM 2

Here is a summary of some facts you should know for Exam 2.

- **Bézout's Theorem** states that if $a, b \in \mathbb{Z}$ and $\gcd(a, b) = d$, then there exist integers $x, y \in \mathbb{Z}$ such that $ax + by = d$. The MOST important case of the theorem is when a, b are *coprime* i.e. $\gcd(a, b) = 1$. In that case, there is a \mathbb{Z} -linear combination of a, b which gives 1 and such a linear combination can be extremely useful. For example:

- **Multiplicative Inverses Modulo m** A congruence class $\{a\}_m$ has an inverse in $(\mathbb{Z}/m\mathbb{Z})^\times$ if and only if $\gcd(a, m) = 1$. To find the inverse, we apply the Euclidean algorithm to a, m to find $x, y \in \mathbb{Z}$ such that $ax + my = 1$. Then, modulo m , my is just "0" so $\{ax\}_m = \{1\}$ or $ax \equiv 1 \pmod{m}$, i.e. x is the inverse of a modulo m or $\{a\}_m^{-1} = \{x\}_m$. Then, if someone asks us to solve $ay \equiv z \pmod{m}$ for y , we can just happily multiply both sides by " a^{-1} " i.e. x to get $xay \equiv xz \pmod{m}$ or $1y \equiv xz \pmod{m}$ i.e. $y \equiv xz \pmod{m}$. For example to solve $7y \equiv 3 \pmod{34}$ I just multiply both sides by 5 to get $y \equiv 15 \pmod{34}$.

- **Zero-Divisors.** If $m \nmid a$ and $\gcd(a, m) > 1$, then $\{a\}_m$ is a **zero-divisor** in $\mathbb{Z}/m\mathbb{Z}$ and $\{a\}_m$ does not have a multiplicative inverse. For $\{a\}_m$ to be a zero-divisor means that $\{a\}_m \neq \{0\}_m$ and that there exists a $\{b\}_m \neq \{0\}_m$ such that $\{ab\}_m = \{0\}$. Thus, $\{21\}_{28}$ is a zero-divisor because $28 \nmid 21$ and $\{21\}_{28}\{4\}_{28} = \{0\}_{28}$.

WARNING: An equation $ay \equiv b \pmod{m}$ where a, b are given and y is a variable does MAY OR MAY NOT have a solution if $\{a\}_m$ is a zero-divisor.

The Chinese Remainder Theorem in Various Guises

The condition $\gcd(m, n) = 1$ plays a very important role because, philosophically speaking, under this condition, a congruence modulo the product mn can be decomposed into two simpler congruences, one modulo m and the other modulo n . A more precise statement is

- **FACT.** If $\gcd(m, n) = 1$, then $x \equiv y \pmod{mn}$ if and only if $x \equiv y \pmod{m}$ and $x \equiv y \pmod{n}$.

- **A Special Case of This Fact.** A very handy special case of this is where $y = 0$ which translates to if $\gcd(m, n) = 1$, then $mn|x$ if and only if $m|x$ and $n|x$. Note that the condition " $m|x$ AND $n|x$ " just means that x is a common multiple of m and n . So what we are saying is that if m, n are coprime then the least (positive) common multiple of m and n is mn and every common multiple of m and n is a multiple of mn .

The above fact leads to the Chinese Remainder Theorem in any one of its versions.

- **CRT Version 1.** If $\gcd(m, n) = 1$, then for any $a, b \in \mathbb{Z}$, the pair of congruences

$$x \equiv a \pmod{m}, x \equiv b \pmod{n}$$

has a solution $x \in \mathbb{Z}$ and this solution is unique in $\mathbb{Z}/mn\mathbb{Z}$ i.e. if x_1, x_2 are any two solutions, then $x_1 \equiv x_2 \pmod{mn}$.

- **CRT Version 2.** A more set-theoretic way of saying it is that we have a well-define map $f : \mathbb{Z}/mn\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ defined by $f(\{x\}_{mn}) = (\{x\}_m, \{x\}_n)$ and that this map is bijective.

- **CRT Version 3.** We can extend CRT VERSION 1 from two congruences to any number of congruences as follows. Suppose m_1, m_2, \dots, m_r are **pairwise coprime** integers, i.e. for any pair $1 \leq i < j \leq r$, $\gcd(m_i, m_j) = 1$. Then for any choice of integers a_1, a_2, \dots, a_r , the family of congruences

$$x \equiv a_i \pmod{m_i}, \quad i = 1, 2, \dots, r$$

has a solution $x \in \mathbb{Z}$ and this solution is unique in $\mathbb{Z}/M\mathbb{Z}$ where $M = m_1 m_2 \dots m_r$ is the product of all the moduli. In other words, if x is one such solution, then the set of all solutions is $\{x + Mk \mid k \in \mathbb{Z}\}$.

- **Algorithm for solving CRT congruences.** Given m_i, a_i as in CRT VERSION 3 above, we DEFINE $n_i = M/m_i$ and we CHOOSE u_i to be multiplicative inverses of the n_i modulo m_i , i.e we choose u_i so that $n_i u_i \equiv 1 \pmod{m_i}$ for $i = 1, \dots, r$. (Notice my notational brilliance here because a “ u ” is just an upside down “ n ”). After all this is done, it’s easy to say what a solution x is, namely ...DRUMROLL...

$$x = n_1 u_1 a_1 + n_2 u_2 a_2 + \dots + n_r u_r a_r.$$

After you get this x , you might have to adjust it by adding multiples of M to it to make it fit the parameters of a problem, such as x being the least positive such solution etc.

Order of elements in $(\mathbb{Z}/m\mathbb{Z})^\times$.

Recall that if $\gcd(a, m) = 1$, then $\text{order}(\{a\}_m) = \min\{k \geq 1 \mid a^k \equiv 1 \pmod{m}\}$. In other words, let’s call an integer k a *neutralizing exponent* for $\{a\}_m$ if raising a to the k th power makes it 1, i.e. renders it “multiplicatively neutral.” How do you like my new less violent language for what I was calling the “killer exponent” in class? Anyway, in words then, the definition of the order is

- The order of $\{a\}_m$ is the LEAST (positive) neutralizing exponent for $\{a\}_m$.
- **Important Fact about Neutralizers** You proved in HW 6, Problem 2(c) that if $\gcd(a, m) = 1$, then $a^k \equiv 1 \pmod{m}$ if and only if $\text{order}(\{a\}_m) \mid k$.
- **Reinterpretation of it:** The set of ALL neutralizing exponents for $\{a\}_m$ is simply the set of all multiples of the LEAST neutralizing exponent.

 Fermat's little Theorem and Euler's generalization of it.

Fermat's little Theorem says that for all integers n , and all primes p , $n^p \equiv n \pmod{p}$. You can think of this as having two cases: $p|n$ and $p \nmid n$. The first case is a no-brainer because in that case n^p and n are both 0 modulo p . Thus, the real content of FLT is the second case where by the existence of the inverse, we can simplify things a bit:

- **FLT:** if $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Euler, who studied Fermat's work very closely, was able to generalize this theorem by consider for an arbitrary integer positive integer m , the function $\varphi(m)$ which just counts how many of the elements of $\mathbb{Z}/m\mathbb{Z}$ are invertible. I should add that by convention $\varphi(1) = 1$. Euler proved the following fact, which maybe we should call "Euler's little Theorem"

- **ELT:** if $\gcd(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

• **Important Consequence.** If we put together the "important fact about neutralizers" mentioned above and ELT, we get that if $\gcd(a, m) = 1$, then

$$\text{order}(\{a\}_m) \mid \varphi(m).$$

A special case of this is that if p is a prime, and $p \nmid a$, then

$$\text{order}(\{a\}_p) \mid (p - 1).$$