```
Math 251, Mon 30-Nov-2020 -- Mon 30-Nov-2020
Discrete Mathematics
Fall 2020


-------------------------------
Monday, November 30th 2020
-------------------------------
Due::   WW RosenCh4Part1 due 11 pm

Other calendar items


-------------------------------
Monday, November 30th 2020
-------------------------------
Wk 14, Mo
Topic:: ~~Chinese remainder theorem~~   Euler totient function

Application of modular arithmetic: pseudorandom number generation     9(b)

Practice: Given these results of Euclidean algorithms carried out
 (a) write the gcd as a linear combination of the original dividend/divisor
 (b) determine whether the divisor has a multiplicative inverse mod the dividend
 1. 330 = 2(156) + 18
    156 = 8(18) + 12
     18 = 1(12) + 6
     12 = 2(6) + 0
    Answer: no multiplicative inverse to 156 in mod 330 arithmetic
            6 = 9(330) - 19(156)


 2. 660 = 15(43) + 15
     43 = 2(15) + 13
     15 = 1(13) + 2
     13 = 6(2) + 1
      2 = 2(1) + 0
    Answer: multiplicative inverse to 43 in mod 660 arithmetic is 307
            1 = 307(43) - 20[660)
```

W.W. 9(b) → like 1, not like 2

$\gcd(330, 156) = 6$

$6 = s(330) + t(156)$

not a problem

$ax + b \equiv c \pmod{m}$

$ax \equiv c - b \pmod{m}$

$156x \equiv c \pmod{330}$ poses difficulties since $\gcd(156, 330) = 6$, not 1.

$\gcd(43, 660) = 1$

$\Rightarrow$ 43 has a mult. inv. mod 660

307 is 43's mult inv. mod 660

$43x \equiv c \pmod{660}$

So, can mult. both sides by 307.

$\neq$

$\equiv$

Some basic facts about linear congruences ax + b \equiv c (mod m)

1. If gcd(a, m) = 1, then there is a single solution x in Z_m $= \{0, 1, \ldots, m-1\}$
2. If gcd(a, m) \ne 1, then

   there might be multiple solutions in Z_m   Note: $\gcd(9, 12) = 3$ (not 1)

   e.g.: 9x \equiv 3 (mod 12) $9x \equiv 3 \pmod{12}$ Solns. in $\mathbb{Z}_{12} = \{0, 1, 2, \ldots, 11\}$

   Answers: 3, 7, 11

   Note: Say 9 has a multiplicative cycle of size 4 mod 12

From a mod 12 mult. table, find x values can be

3: since $9(3) = 27 \equiv 3 \pmod{12}$

7: since $9(7) = 63 \equiv 3 \pmod{12}$

11: since $9(11) = 99 = 3 \pmod{12}$

15 is redundant since $15 \equiv 3 \pmod{12}$ and 3 is already listed as an answer

   e.g.: 286x \equiv 130 (mod 442)

   Answers: 2, 19, 36, 53, 70, 87, 104, 121, 138, ..., 410, 427

   Note: Say 286 has a multiplicative cycle of size 4

$286x \equiv 130 \pmod{442}$ $\gcd(442, 286) = 26$ (not 1)

mod 442 mult table is unwieldy

Another approach (see below)

   there might be no solution in Z_m

   e.g.: 9x \equiv 4 (mod 12) $9x \equiv 4 \pmod{12}$

$\gcd(9, 12) = 3$ (I don't expect exactly one soln.)

$9x \equiv 4 \pmod{12} \implies 12 \mid 9x - 4$

or $12k = 9x - 4$

Can take gcd (3) out of both

But $3 \nmid 4$

$\implies$ no solution

Prime numbers and their properties

Definition 1: An integer $p \geqslant 2$ is said to be **prime**, whenever some $n \in \mathbb{Z}^+$ satisfies $n \mid p$, then $n = 1$ or $n = p$. If $p \geqslant 2$ is not prime, then it is called **composite**.

Various facts about prime numbers can be deduced, some easily, some not so easily.

1. **Fundamental Theorem of Arithmetic**: Every positive integer $n \geqslant 2$ is either prime or the product of primes. Up to the order of the factors, the prime factorization of n is unique, and takes the form $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.

   We proved the first sentence in this theorem earlier in the semester, using *strong induction*.

2. There are infinitely many primes.

   Euclid, who lived some 300 years before Christ, gave an elegant proof of this fact, which goes something like this: If there were only finitely many primes, the full list would make up the finite set $S = \{p_1, p_2, \ldots, p_N\}$, with each $p_{j-1} < p_j$. From these, we can form the number

   $$M = p_1 p_2 p_3 \cdots p_N + 1,$$

   which is not in S, as it is larger than S's largest element, p_N. So, M, not a prime itself, is composite, the product of primes. But as no prime in S divides M, the primes that make up M show that S must not have contained all primes. In other words, we have arrived at a contradiction that the set S simultaneously contains all primes, and does not contain the primes dividing M. The reason we have arrived at this contradiction is that our original assumption, that there are only finitely many primes, is false.

3. If p is prime, then $\forall n \in \mathbb{Z}^+$, $\gcd(n, p) = 1$ or $\gcd(n, p) = p$.

4. If p is prime, $a_1, a_2, \ldots, a_n$ are positive integers, and $p \mid a_1 a_2 \cdots a_n$, then there is at least one a_i for which $p \mid a_i$.

5. Suppose $n \geqslant 2$ is an integer, and suppose that, for each $k = 2, 3, \ldots, \lfloor \sqrt{n} \rfloor$, $k \nmid n$. Then n is prime.

   In particular, in checking that $n = 131$ is prime, we can verify $2 \nmid 131$, $3 \nmid 131$, $5 \nmid 131$, $7 \nmid 131$, and $11 \nmid 131$. Since $\lfloor \sqrt{131} \rfloor = 11$, we need go no further, and can declare 131 is prime. The reason we can stop is that, if there were a larger integer m which divided 131, then the other integer k for which $mk = 131$ would be smaller than $\lfloor \sqrt{131} \rfloor$, and would have been found already.

6. **Prime Number Theorem**. For each integer $n \geqslant 2$ define $\pi(n) = \left| \{p \leqslant n \,|\, p \text{ is prime}\} \right|$. The ratio $\pi(n)/n$ gives the *density* of primes in the set of positive integers up to and including n. This ratio is asymptotic to $1/\ln(n)$ as $n \to \infty$.

   Thus, in the first 10^{1000} integers only about 1/2302.6 integers have been prime. Out to 10^{10000}, only about 1/23026 have been.

7. **Fermat's Little Theorem**. If p is prime and a is an integer not divisible by p, then
$$a^{p-1} \equiv 1 \pmod{p}.$$
   Moreover, for *every* integer b,
$$b^p \equiv b \pmod{p}.$$
   The consequences of Fermat's Little Theorem include these:
   - When doing arithmetic $\bmod p$ (a prime), it becomes much simpler to raise integers to powers. Say our modulus is 11. Then
$$6^{502} = (6^{500})(6^2) = (6^{10})^{50}(36) \equiv (1)(36) \equiv 3 \pmod{11}.$$
   - If p is prime and $p \nmid a$, then the multiplicative inverse of $a \pmod{p}$ is a^{p-2}.
   - If it happens that $\gcd(a, n) = 1$ and $a^{n-1} \not\equiv 1 \pmod{n}$, then n is not prime.
     Alternatively, if $a^n \not\equiv a \pmod{n}$, then n is not prime.
     As an illustration of this,
$$2^{91} = (2^{12})^7(2^7) \equiv (1)^7(128) \equiv 37 \pmod{91}.$$
     Thus, 91 is composite for, if it were prime, then this last statement would have been of equivalence with $1 \pmod{91}$, not $37 \pmod{91}$.
8. The **Euler totient function** $\varphi(n)$ counts the number of integers $1 \leqslant a \leqslant n$ such that $\gcd(a, n) = 1$. When n is
   - a prime ($n = p$), $\varphi(p) = p - 1$.
   - the power of a prime ($n = p^\alpha$), $\varphi(p^\alpha) = \left(1 - \frac{1}{p}\right) p^\alpha$.

   It is also the case that, whenever $\gcd(a, b) = 1$, $\varphi(ab) = \varphi(a)\varphi(b)$. Taken together with the above, this tells us generally that, given the prime factorization
$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \qquad \text{we have} \qquad \varphi(n) = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) n.$$

There is this generalization of Fermat's Little Theorem.

Theorem 1 (Euler's Theorem): For positive integers a, n with $\gcd(a, b) = 1$, $a^{\varphi(n)} \equiv 1 \pmod{n}$.