First Results in Elementary Number Theory

1. **Definition.** Let a and b be two integers, not both zero. We say that d is a *common divisor* of a and b if
$$d \mid a \qquad \text{and} \qquad d \mid b.$$
Note that the common divisors of a and b are no larger than the maximum of $|a|$ and $|b|$. So it is natural to consider the following.

2. **Definition.** The *greatest common divisor* of a and b is the greatest (largest) of the common divisors of a and b. It is denoted by $\gcd(a, b)$.

3. **Proposition.** If $d \mid a$ and $d \mid b$, then $d \mid (xa + yb)$ for all $x, y \in \mathbb{Z}$.

   We proved this earlier in class. We say that if d divides both a and b, then d divides any *integer linear combination* of a and b.

   This leads to a lovely recursive algorithm for finding greatest common divisors.

4. **Proposition [Euclidean Algorithm].** Let a and b be integers and b positive. By the Division Algorithm there are unique integers q, r so that
$$a = bq + r \qquad \text{and } 0 \le r < b.$$
Then
$$\gcd(a, b) = \gcd(b, r).$$

5. **Implementing the Euclidean Algorithm.** One starts with integers a and b with $b > 0$.

   - Find integers q_1, r_1 such that
   $$a = bq_1 + r_1 \qquad \text{and } 0 \le r_1 < b$$
   Proposition 1 above ensures that
   $$\gcd(a, b) = \gcd(b, r_1).$$
   - Find integers q_2, r_2 such that
   $$b = r_1 q_2 + r_2 \qquad \text{and } 0 \le r_2 < r_1$$
   Proposition I above ensures that
   $$\gcd(b, r_1) = \gcd(r_1, r_2).$$
   - Stop when you obtain a remainder of 0. Suppose you have integers r_k, r_{k+1} and the DA gives
   $$r_k = r_{k+1} q_{k+2} + 0$$
   Then $\gcd(r_k, r_{k+1}) = r_{k+1}$, and the previous steps combine to give
   $$r_{k+1} = \gcd(r_k, r_{k+1}) = \cdots = \gcd(b, r_1) = \gcd(a, b).$$

6. **Proposition (Bezout's identity).** Let a, b be integers, not both zero. Then there exist integers l, m such that

$$\gcd(a,b) \;=\; la + mb.$$

This can be proven either by performing a sequence of backward substitutions in the Euclidean Algorithm or by the lovely application of the Least Principle that we saw in class.

This has the following consequences.

7. **Proposition.** Let a, b, c be integers. If $\gcd(a,b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof. The hypothesis that $\gcd(a,b) = 4$ and Bézout's identity imply that there exists integers r, s so that

$$ra + sb \;=\; 1.$$

Multiplying across by c gives

$$rac + sbc \;=\; c.$$

Now $a \mid a$ (since $a = a(1)$) and that $a \mid bc$ by hypothesis. Hence the proposition in item 3 above implies that a divides the following integer linear combination of a and bc

$$rc(a) + s(bc)$$

This means that $a \mid c$. □

8. **Corollary (Euclid's Lemma).** Let p, b, c be integers, and p a prime number. If $p \mid bc$ and $p \nmid b$, then $p \mid c$.

Proof. This follows from the previous proposition and the following observation. Since p is prime, if $p \nmid b$, then $\gcd(p,b) = 1$. This is because the only positive factors of p are p and 1, and since p is not a factor of b, then the only positive factor they have in common is 1. Hence $\gcd(p,b) = 1$. □

This result can also be phrased as follows. *If a, b are integers, p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.*

9. **Definition.** Two integers a and b are said to be *relatively prime* if $\gcd(a,b) = 1$.

The proposition in item 7 above is often stated as follows "if $a \mid bc$ and a is relatively prime to b, then $a \mid c$." Note that if p is a prime number and b is an integer and $p \nmid b$, then p and b are relatively prime. This is why Euclid's Lemma follows from the proposition in item 7.

10. **Lemma.** If $p, q_1, \ldots, q_n$ are all primes and

$$p \mid q_1 \ldots q_n$$

then $p = q_j$ for some $1 \leq j \leq n$.

Proof. We argue by induction on n.

The base case $n = 1$ is seen to be true as follows. If p and q_1 are both primes, then $p \mid q_1$ implies $p = q_1$. This is because the only factors of q_1 are q_1 and 1 (because q_1 is prime), and $p \neq 1$ (because p is prime).

Assume it is true for case k. That is given primes $p, q_1, \ldots, q_k$ if $p \mid q_1 \ldots q_k$, then $p = q_j$ for some $1 \leq j \leq k$. Now given primes $p, q_1, \ldots, q_{k+1}$ with the property that $p \mid q_1 \ldots q_{k+1}$. Denoting $q_1 \ldots q_k$ by b and q_{k+1} by c, our condition becomes $p \mid bc$. Euclid's Lemma implies that $p \mid b$ or $p \mid c$. In the case $p \mid b$, then $p \mid q_1 \dots q_k$ and so $p = q_j$ for some $1 \le j \le k$ by the induction hypothesis. In the case $p \mid c$, then $p \mid q_{k+1}$ and so $p = q_{k+1}$ by the base case argument. In either case we have shown $p = q_j$ for some $1 \le j \le (k+1)$.

By the principle of induction the theorem holds for all positive integers n. □

11. **Theorem (Fundamental Theorem of Arithmetic).** Every integer a greater than or equal to 2 can be expressed as a product of prime numbers. That is

$$a \;=\; p_1 \dots p_n$$

where the p_j are primes. This includes the special case of $n = 1$ and so a is prime.

Furthermore, this expression is unique if we require that the primes be listed in non-decreasing order.

$$p_1 \;\le\; p_2 \;\le\; \cdots \;\le\; p_n.$$

Proof. We have seen the proof of existence already (as an example of Strong Induction). So we only need to argue uniqueness. Let us establish the following form of the uniqueness statement by Strong Induction.

If the integer $n \ge 2$ is a product of prime numbers

$$p_1 \dots p_r \;=\; n \;=\; q_1 \dots q_s$$

where the primes p_i and q_j are arranged in non-decreasing order, then

$$r \;=\; s \quad \text{and} \quad p_i = q_i \quad \text{for all } 1 \le i \le r.$$

Base case. The statement is clearly true for the base case $n = 2$. This is because 2 is prime and so has a unique expression as a product of primes; that is, $r = s = 1$ and $p_1 = q_1 = 2$.

Induction step. Suppose that the uniqueness result above is true for all integers between 2 and k. Consider the integer $(k+1)$. Either $(k+1)$ is prime, in which case the uniqueness statement holds exactly as in the base case (that is, $r = s = 1$ and $p_1 = q_1 = (k+1)$), or $(k+1)$ is composite and we can write

$$p_1 \dots p_r \;=\; (k+1) \;=\; q_1 \dots q_s$$

where $r \ge 2$. Then $p_1 \mid q_1 \dots q_s$ and the Lemma implies that $p_1 = q_j$ for some $1 \le j \le s$. Delete p_1 from both sides gives

$$p_2 \dots p_r \;=\; \frac{(k+1)}{p_1} \;=\; q_1 \dots q_{j-1} q_{j+1} \dots q_s$$

But $\frac{(k+1)}{p_1}$ is an integer in the range $2, \dots, k$ and so the induction hypotheses implies $r - 1 = s - 1$ and that $p_i = q_i$ after rearranging the q_i in nondecreasing order. Therefore $r = s$ and $p_i = q_i$ after appropriate relabeling of the q's.

Thus the uniqueness statement holds by the principle of strong induction. □

12. **Applications of the Fundamental Theorem.**

(a) Relationship between product, gcd and lcm. Given integers a, b

$$ab = \gcd(a, b)\text{lcm}(a, b)$$

where $\text{lcm}(a, b)$ is the *least common multiple* of a and b.

(b) Fractions in least terms and irrationality of square roots in case one of numerator or denominator is not a perfect square.

(c) Irrationality of $\log_p(q)$.

(d) $\gcd(a, b_i) = 1$ for $1 \leq i \leq k$ iff $\gcd(a, \prod_{i=1}^{k} b_i) = 1$.

(e) $a_i \mid n$ for $1 \leq i \leq k$ and $\gcd(a_i, a_j) = 1$ for all $i \neq j$, then $(a_1 \dots a_k) \mid n$.

13. **Theorem (Euclid).** There are infinitely many prime numbers.

Proof. We argue by contradiction. Suppose that there are only finitely many prime numbers. List them

$$p_1, \dots, p_n$$

Now consider the number $N = p_1 \dots p_n + 1$. Note that none of the primes p_i is a factor of N, since N is constructed so that there is a remainder of 1 on division by each p_i.

Therefore, the prime factors of N are all distinct from the p_i. This contradicts the fact that $p_1, \dots, p_n$ was a complete list of all primes. □

14. **Exercise.** Prove that there are infinitely many prime numbers which are congruent to 3 mod 4.

Hint. In Euclid's proof we considered a product plus 1. Think about 1 plus 2 times a product.

15. **Size of primes.** The nth prime number p_n satisfies $p_n \leq 2^{2^{n-1}}$ for all $n \in \mathbb{N}$.

Proof. We argue by strong induction. The first prime is 2 and

$$2 \leq 2^1 = 2^{2^{1-1}}$$

Therefore the base case is proven.

The induction hypothesis is that the jth prime satisfies

$$p_j \leq 2^{2^{j-1}}$$

for $1 \leq j \leq k$.

Looking closely at Euclid's proof that there are infinitely many primes, we see that

$$p_{k+1} \leq p_1 \dots p_k + 1 \leq (2)(2^{2^1})(2^{2^2}) \cdots (2^{2^{k-1}}) + 1 \leq 2^{2^k - 1} + 1 \leq 2^{2^k}.$$

Therefore, the result holds by the principle of strong induction. □

16. **Proposition.** If p is a prime number, then every non-zero element of $\mathbb{Z}_p$ has a multiplicative inverse.

Proof. Let a be a nonzero number in $\mathbb{Z}_p$. This means $1 \leq a \leq (p - 1)$. Therefore, since p is prime, we have $\gcd(a, p) = 1$.

Bezout's identity implies that there are integers x, y so that

$$1 \; = \; ax + py$$

This means that $ax \equiv 1 \mod p$, and so a has a multiplicative inverse in $\mathbb{Z}_p$. □

We shall use the notation $\frac{1}{a}$ to denote the multiplicative inverse of $a \mod p$. Just keep in mind that $\frac{1}{a}$ is some integer in $\{1, \ldots, p-1\}$.

17. **Theorem 8 (Fermat's Little Theorem).** Let p be a prime number and let a be a nonzero element of $\mathbb{Z}_p$. Then

$$a^{p-1} \; \equiv \; 1 \mod p.$$

Proof. Now a belongs to the list of numbers $1, 2, \ldots, (p-1)$. Consider the list of numbers

$$a(1), a(2), \ldots, a(p-1) \qquad\qquad (*)$$

all computed $\mod p$. We claim that the list $(*)$ is the same as **all of** the numbers on the original list $1, 2, \ldots, (p-1)$ after some rearranging.

Proof of claim. We argue by contradiction. Suppose that the list $(*)$ is not a rearrangement of **all of** the numbers on the standard list $1, 2, \ldots, (p-1)$. Now since we are computing values $\mod p$, the numbers in the list $(*)$ above all belong to the list $1, 2, \ldots, (p-1)$. Since it is not a rearrangement of the standard list $1, 2, \ldots, (p-1)$, there must be some numbers missing. By the pigeonhole principle there are values $1 \leq x \neq y \leq (p-1)$ for which $ax = ay$ (two distinct letters x and y get sent to the same pigeonhole $ax = ay$). Now, the previous proposition implies that a has a multiplicative inverse $\frac{1}{a}$. But then we obtain $\frac{1}{a}ax = \frac{1}{a}ay$ or $x = y$ and this contradicts $x \neq y$. This proves the claim.

Now since, $a(1), \ldots, a(p-1)$ is just a rearrangement of $1, 2, \ldots, (p-1)$ they have the same product

$$a(1)a(2)\cdots a(p-1) \; \equiv \; (1)(2)\cdots(p-1) \mod p$$

or in other words

$$(1)(2)\cdots(p-1)a^{p-1} \; \equiv \; (1)(2)\cdots(p-1) \mod p.$$

Again, the previous proposition implies that each nonzero j has a multiplicative inverse (denoted by $\frac{1}{j}$) and so we can write

$$\frac{1}{1}\frac{1}{2}\cdots\frac{1}{p-1}(1)(2)\cdots(p-1)a^{p-1} \; \equiv \; \frac{1}{1}\frac{1}{2}\cdots\frac{1}{p-1}(1)(2)\cdots(p-1) \mod p$$

which simplifies out to give

$$a^{p-1} \; \equiv \; 1 \mod p. \quad \Box$$

18. **Exercise/Application.** We have proven explicitly in the special cases when $m = 2, 3, 5, 7, 11$ that $m \mid (a^m - a)$ for all integers a. Show that Fermat's Little Theorem tells us that if p is a prime number, then $p \mid (a^p - a)$ for all integers a.

We also saw in class notes that there were examples of integers n where $4 \nmid (n^4 - n)$, and examples where $6 \nmid (n^6 - n)$ etc. You might be tempted to conclude that

$$(p \mid (n^p - n) \text{ for all integers } n) \qquad \text{if and only if} \qquad p \text{ is a prime number.}$$

Fortunately, the universe is **not** so accommodating (and so is much more interesting!). Google the term "Carmichael number."

19. **Exercise/Application 2.** Compute the following huge powers in modular arithmetic, and prove that the statements about modular exponents are correct:
$123456^{7891011} \mod 11$.
$3^{256} \mod 7$.
$7^{85} \mod 41$.
$5^{223} \mod 23$.
If p is prime, then $a^b \equiv (a \mod p)^{(b \mod p-1)} \mod p$.
If p and q are distinct primes and $\gcd(a, pq) = 1$, then $a^{(p-1)(q-1)} \equiv 1 \mod pq$.
$3^{123} \mod 35$. (Hint: Note that $35 = (5)(7)$.)
$7^{2763} \mod 143$. (Hint: What are the factors of 143?)

20. **Hint on Exercise.** Start with distinct primes p and q, and any integer a satisfying $\gcd(a, pq) = 1$. Show that $p \nmid a$ and show that $q \nmid a$.

    Since $p \nmid a$, we know from Fermat's little theorem that $a^{p-1} \equiv 1 \mod p$. What can you say about $a^{(p-1)(q-1)} \mod p$? Rephrase this so that it is a statement about some number being divisible by p.

    Since $q \nmid a$, we know from Fermat's little theorem that $a^{q-1} \equiv 1 \mod q$. What can you say about $a^{(q-1)(p-1)} \mod q$? Rephrase this so that it is a statement about some number being divisible by q.

    Show how to use the results of the previous 2 paragraphs to obtain the conclusion $a^{(p-1)(q-1)} \equiv 1 \mod pq$.

21. **Pigeonhole Principle.** If $n \geq 2$ letters are distributed into $m < n$ (and $m \geq 1$) mailboxes (pigeonholes), then at least two letters end up in the same mailbox.

    Proof. We note that the general statement follows from the following statement.
    P(n): *If $n \geq 2$ letters are distributed among $(n-1)$ pigeonholes, then one pigeonhole will contain at least two letters.* This is because we can think of distributing n letters among $m < n$ pigeonholes as being the same as distributing the letters among $(n-1)$ pigeonholes where $(n-1) - m$ of the pigeonholes sealed up.

    The base case consists of $n = 2$ letters being distributed into 1 pigeonhole. This one pigeonhole ends up with both letters.

    Assume that the result is true for case $n = k$. That is if k letters are distributed into $k-1$ pigeonholes, then a pigeonhole ends up with at least two letters. Now given $k+1$ letters and k pigeonholes, pick a pigeonhole at random. It has 0, 1 or at least 2 letters in it. If it has at least 2 letters in it, then we have a pigeonhole with at least two letters, and we are done. If it has 1 letter in it, we can now see that the remaining k letters have been distributed into $k-1$ pigeonholes, and the existence of a pigeonhole with at least two letters is guaranteed by the induction hypothesis. Finally, if it has 0 letters, then the $k+1$ letters (and therefore any k sub collection of these letters) are being distributed into $k-1$ pigeonholes, and again the induction hypothesis guarantees that one of these $k-1$ pigeonholes contains at least 2 letters. In all three cases, we have shown that $P(k+1)$ is true.

    The result now follows by the principle induction. □

    The pigeonhole counting principle is used in the proof of Fermat's Little Theorem.

22. **Proposition.** $ca \equiv cb \mod m$ if and only if $a \equiv b \mod \frac{m}{\gcd(c,m)}$.

Proof. One direction is immediate. If $a \equiv b \mod \frac{m}{\gcd(c,m)}$, then $\frac{m}{\gcd(m,c)} \mid (b-a)$. This means that $(b-a) = \frac{m}{\gcd(m,c)}q$ for some integer q. Multiplying across by c gives

$$c(b-a) \;=\; c\frac{m}{\gcd(m,c)}q \;=\; m\frac{c}{\gcd(m,c)}q$$

But $\frac{c}{\gcd(m,c)}$ is an integer, and so $m \mid c(b-a)$ or $ca \equiv cb \mod m$.

Proving the reverse direction uses a previous result. If $ca \equiv cb \mod m$, then $m \mid c(b-a)$ and so $c(b-a) \;=\; mx$ for some integer x. Dividing across by $\gcd(m,c)$ gives

$$\frac{c}{\gcd(m,c)}(b-a) \;=\; \frac{m}{\gcd(m,c)}x$$

This means that $\frac{m}{\gcd(m,c)} \mid \frac{c}{\gcd(m,c)}(b-a)$. But $\frac{m}{\gcd(m,c)}$ and $\frac{c}{\gcd(m,c)}$ are relatively prime, and so the proposition in item 7 implies that $\frac{m}{\gcd(m,c)} \mid (b-a)$. That is $a \equiv b \mod \frac{m}{\gcd(m,c)}$. □

23. **Theorem (Linear Congruences).** The congruence equation $ax \equiv b \mod m$ has a solution if and only if $\gcd(a,m) \mid b$.

    If x_0 is one solution, then the complete list of all solutions is given by

    $$x_0 + k\frac{m}{\gcd(a,m)} \qquad \text{for } 0 \le k \le \gcd(a,m)-1.$$

    Proof. If $ax \equiv b \mod m$ has a solution, then $b - ax = mq$ for some integers x and q. Therefore b is an integer linear combination of a and m, and so $\gcd(a,m) \mid b$.

    Conversely, if $\gcd(a,m) \mid b$, then $b = \gcd(a,m)w$ for some integer w. Bezout's identity tells us that $\gcd(a,m) = ra + sm$ for some integers r, s. Combining gives

    $$b \;=\; \gcd(a,m)w \;=\; (ra+sm)w \;=\; a(rw) + m(sw)$$

    This means that $b - a(rw)$ is divisible by m, and so $a(rw) \equiv b \mod m$.

    Finally, if x and x_0 are two solutions of $ax \equiv b \mod m$ then $a((x-x_0) \equiv 0 \mod m$. This means $a(x-x_0) = mp$ for some integer p. Dividing across by $\gcd(a,m)$ gives

    $$\frac{m}{\gcd(a,m)} \mid \frac{a}{\gcd(a,m)}(x-x_0)$$

    and so (by the proposition in item 7) $\frac{m}{\gcd(a,m)} \mid (x-x_0)$. This gives the solution

    $$x \;=\; x_0 + k\frac{m}{\gcd(a,m)} \qquad \text{for } k = 0, 1, 2 \ldots$$

24. **Theorem (Simultaneous Congruences — Chinese Remainder Theorem).** The following puzzle appears in the Brahma-Sphuta-Siddhanta (Brahma's Correct System) by Brahmagupta (born 598 AD):

    An old woman goes to market and a horse steps on her basket and crushes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, *but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?*

Theorem (Chinese Remainder Theorem). Let $m_1, \dots, m_k$ be pairwise relatively prime natural numbers. The system of simultaneous linear congruences

$$x \equiv a_1 \mod m_1\,, \;\; \dots \;\; , x \equiv a_k \mod m_k$$

has a unique solution $\mod M$, where $M = m_1 \dots m_k$.

Proof. We establish existence of a solution first. Indeed, let $z_i = M/m_i$ and note that for each i the congruence

$$z_i y_i \equiv 1 \mod m_i$$

has a solution y_i (because $\gcd(z_i, m_i) = 1$). Now set

$$x \;=\; a_1 y_1 z_1 + \dots + a_k y_k z_k$$

Note that $m_i \mid z_j$ when $i \neq j$. Therefore $x \equiv 0 + \cdots 0 + a_i y_i z_i + 0 + \cdots + 0 \mod m_i$. But we found the y_i so that $y_i z_i \equiv 1 \mod m_i$. Thus $x \equiv a_i y_i z_i \equiv a_i \mod m_i$.

Now for uniqueness. If x and y are two solutions, then $x - y \equiv 0 \mod m_i$ for each i. This means $m_i \mid (x-y)$ for all i. But the m_i are pairwise relatively prime. Thus $(m_1 \dots m_k) \mid (x-y)$. This means $M \mid (x - y)$ or in other words $x \equiv y \mod M$. □

25. **The number of eggs problem.** We rewrite the statements about the (as yet unknown) quantity x of eggs in modern congruence notation.

    - $x \;\equiv\; 1 \mod 2$
    - $x \;\equiv\; 1 \mod 3$
    - $x \;\equiv\; 1 \mod 4$
    - $x \;\equiv\; 1 \mod 5$
    - $x \;\equiv\; 1 \mod 6$
    - $x \;\equiv\; 0 \mod 7$

    Unfortunately not all of the m_k are relatively prime (e.g., 2, 4, 6 all have 2 in common). However, the first congruence just tells us that x is an odd number, so we can eliminate this congruence, because $x \equiv 1 \mod 4$ will guarantee oddness. We also remove the congruence $x \equiv 1 \mod 6$ because 6 has factors in common with 4 and 3. We will manually check if our solution satisfies $x \equiv 1 \mod 6$. This leaves us with

    - $x \;\equiv\; 1 \mod 3$
    - $x \;\equiv\; 1 \mod 4$
    - $x \;\equiv\; 1 \mod 5$
    - $x \;\equiv\; 0 \mod 7$

    where 3, 4, 5, 7 are all pairwise relatively prime.

    Next, we work through the steps of the CRT. Let $M = (3)(4)(5)(7) = 420$ and

    (a) let $z_1 = (4)(5)(7) = 140$, $z_2 = (3)(5)(7) = 105$, $z_3 = (3)(4)(7) = 84$, $z_4 = (3)(4)(5) = 60$.

(b) Next, solve for multiplicative inverses

$$\begin{aligned} y_1 &= \frac{1}{140} = \frac{1}{2} = 2 \mod 3 \\ y_2 &= \frac{1}{105} = \frac{1}{1} = 1 \mod 4 \\ y_3 &= \frac{1}{84} = \frac{1}{4} = 4 \mod 5 \\ y_4 &= \frac{1}{60} = \frac{1}{4} = 2 \mod 7 \end{aligned}$$

(c) Now use the formula in the CRT.

$$x = a_1y_1z_1+a_2y_2z_2+a_3y_3z_3+a_4y_4z_4 = (1)(2)(140)+(1)(1)(105)+(1)(4)(84)+(0)(2)(60) = 721.$$

(d) Finally we have $x = 721 \mod 420$ or in other words $x = 301$. Since $301 \equiv 1 \mod 6$ the final congruence relation is also satisfied. The minimum number of eggs is 301.