Appendix G: GCD, mod n, totient φ(n), Euler Theorem, Fermat's Little Theorem

Here we take a brief tour of "number theory" with the goal being to arrive at the endpoints of Euler's Theorem (Fact 11) and Fermat's Little Theorem (Fact 12). More trees in the forest. The entire thread presented here (excluding a few references to items in the main document) is completely self-contained, and each Fact has a proof. In our selected pathway, every Fact in this section is required to get the train to the station. No doubt there are shorter paths, but all these Facts are worth stating and proving. If the GCD and Mod concepts are old hat to you, all these Facts will all be familiar.

Euler's Theorem is used in Appendix E to prove (E.1).

The final two Facts 13 and 14 (the coda) show how the number of primitive elements and the number of primitive polynomials of a Galois Field are related to the totient function φ defined below in (G.14).

Fact 0: These fundamental modulo arithmetic rules were stated and derived in (1.31b) :

$$(x+y+z+\ldots) \bmod n = ([x \bmod n] + [y \bmod n] + [z \bmod n] + \ldots) \bmod n$$

$$(x*y*z+\ldots) \bmod n = ([x \bmod n] * [y \bmod n] * [z \bmod n] + \ldots) \bmod n \qquad \textit{(1.31b)}$$

Fact 1: Let d = GCD(c,m). Then by the meaning of "common divisor" there must exist integers N_1 and N_2 such that $c/d = N_1$ and $m/d = N_2$. The fact claims that $GCD(N_1,N_2) = 1$. (G.1)

Proof: Suppose $GCD(N_1,N_2) = K > 1$. Then there must exist integers M_1 and M_2 such that

$N_1/K = M_1$	$\Rightarrow N_1 = M_1K$	$\Rightarrow c/d = M_1K$	$\Rightarrow c/(dK) = M_1$
$N_2/K = M_2$	$\Rightarrow N_2 = M_2K$	$\Rightarrow m/d = M_2K$	$\Rightarrow m(dK) = M_2$.

The equations on the right show that then dK > d is a common divisor of c and m which is a contradiction since d is supposed to be the largest common divisor. QED.

Fact 2: Suppose $GCD(N_1,N_2) = 1$ and $N_1A = N_2B$. Then N_2 divides A and N_1 divides B. (G.2)

Proof:

- If $N_1 = 1$ then $A = N_2B$ so N_2 divides A and of course $N_1 = 1$ divides B.
- If $N_2 = 1$ then $B = N_1A$ so N_1 divides B and of course $N_2 = 1$ divides A.

- If $N_1>1$ and $N_2> 1$ and if $N_1A = N_2B$, then N_2 divides N_1A (quotient B). But if $GCD(N_1,N_2) = 1$, N_2 cannot divide N_1 because if it did then $N_2 > 1$ would be a common divisor of N_1 and N_2. Thus, if N_2 divides N_1A then N_2 must be dividing A. Similarly, N_1 must divide B.

Notation: The notation a = b mod m is a *shorthand* for a mod m = b mod m, or (a-b) mod m = 0. It means that a and b are congruent mod m. The notation is a little misleading since it seems to say for example 100 = 100 mod 4 = 0 so 100 = 0, but that is not what it means. It means that 100 is congruent with 0 mod 4. A better notation might be a = b (mod m), but that adds clutter. Note then that for a and b integers in Z, there exists an integer I such that

$$a = b \bmod m \Leftrightarrow a \bmod m = b \bmod m \Leftrightarrow (a-b) \bmod m = 0 \Leftrightarrow (a-b) = I\,m \Leftrightarrow a = b + I\,m \qquad (G.3)$$

Fact 3: $ca = cb \bmod m \Leftrightarrow a = b \bmod \frac{m}{GCD(c,m)}$ (G.4)

Proof: Let $d \equiv GCD(c,m)$. As in **Fact 1**, there exist N_1 and N_2 such that

$c = N_1 d$

$m = N_2 d \Rightarrow \frac{m}{GCD(c,m)} = \frac{m}{d} = N_2$ = an integer (which is promising!)

Proof in the $\Rightarrow$ direction:

$$ca = cb \bmod m \Rightarrow ca = cb + em \Rightarrow c(a-b) = em \Rightarrow N_1 d(a-b) = em \Rightarrow a-b = \frac{em}{N_1 d} = \frac{e}{N_1}\frac{m}{d}.$$

If we can show that $\frac{e}{N_1}$ is an integer, then we have shown that $a = b \bmod \frac{m}{d}$ as claimed. Go back to

$$N_1 d(a-b) = em \Rightarrow N_1(a-b) = e\frac{m}{d} \Rightarrow N_1(a-b) = N_2\, e\,.$$

Since $GCD(N_1,N_2) = 1$ by **Fact 1**, **Fact 2** says that N_2 divides (a-b). Now write the last equation as

$$\frac{e}{N_1} = \frac{a-b}{N_2}$$

Since we just showed that N_2 divides a-b, we have shown that $\frac{e}{N_1}$ is an integer, QED.

Proof in the $\Leftarrow$ direction:

If $a = b \bmod N_2$ then $a = b + kN_2$ and $ca = cb + ckN_2$. But

$$ckN_2 = (N_1 d)k\,\frac{m}{d} = (N_1 k)m$$

Thus $ca = cb + (N_1 k)m$ and so $ca = cb \bmod m$. QED.

Corollary 3. If GCD(c,m) = 1 then [$ca = cb \bmod m \Leftrightarrow a = b \bmod m$] . (G.5)

In this special case of **Fact 3**, if we see ca = cb, we can divide both sides by c to get $a = b \bmod m$.

Fact 4: (Linear Congruence Theorem).
If $ax = b \bmod m$ and GCD(a,m) = 1, there is a unique mod-m solution x. (G.6)

Comment: If a = b mod m, then a and b are said to be **congruent** mod m. The set of integers a which are congruent to b mod n is called a **congruence class**. The set of such values was called a residue class in our residue class ring discussion of Chap 1 (c), with an example shown in (1.32). In this Fact our equation to be solved is ax = b which is a linear equation and ax is congruent to b mod m, hence the theorem name.

History: An equation of two of more variables, like $ax^2 + by + cy^3 + dz = e$, in which all coefficients and variables are restricted to be integers, is called a **Diophantine equation**, named after a Greek algebra guy Diophantus circa 250 BC. An equation like ax + by = c is a linear Diophantine equation. We saw an example of this in (1.43), Bezout's Identity $d = x\,n_1 + y\,n_2$ where $d = GCD(n_1,n_2)$ and we want to solve for integers x and y. In our current Fact 4, we have $ax = b \bmod m$ which is a "linear Diophantine equation mod m". Hilbert's 10th Problem (1900) was to find an algorithm which could determine whether a given Diophantine equation has a solution or not. The work of several people from 1944 to 1970 showed that such an algorithm does not exist for the general case.

Proof of Fact 4: We want to solve $ax = b \bmod m$ for x. Consider the linear Diophantine equation

$ay - mz = 1$ $\quad 1 = GCD(a,m)$ $\quad$ variables y,z

Since this is the **Bezout Identity (1.43)**, we know there exists an integer solution for y and z. So we have a specific value of y. Multiply by b to get

$a(by) = b + m(bz) \Rightarrow a(by) = b \bmod m$

Thus our solution is x = by. Suppose there were another solution x'. Then

$ax = b \bmod m$
$ax' = b \bmod m \Rightarrow ax = ax' \bmod m$

Since GCD(a,m) = 1, **Corollary 3** says that x = x' mod m. Thus our solution x = by is the only solution mod m. **QED**

Corollary 4: Element a of Z_m has an inverse if GCD(a,m) = 1. (G.7)

Proof: In **Fact 4** we showed that in this case ax = b mod m had a unique solution. Setting b = 1 we find that ax = 1 has a unique solution. But that solution is a^{-1}. [Z_m means Mod(m, +, •)].

Fact 5: Given a,b > 0, and if x and y exist such that ax+by = 1, then gcd(a,b) = 1. (G.8)

Proof: Suppose gcd(a,b) = Q > 1. Then

$a = QN_1$
$b = QN_2$ => $1 = ax+by = (QN_1)x + (QN_2)y = Q(N_1x + N_2y)$ => $1/Q = N_1x + N_2y$.

But since Q > 1, this says fraction = integer which is a contradiction, so Q = 1.

Fact 6: If gcd(a,m) = 1 and gcd(b,m) = 1, then gcd(ab,m) = 1. (G.9)

Proof: From the if conditions we know from **Bezout's Identity (1.43)** that x,y,x',y' exist such that

$1 = ax + my$ and $1 = bx' + my'$.

Thus,

$1 = (ax + my)(bx' + my') = ab(xx') + m(ybx'+axy'+myy') = ab\,x'' + m\,y''$.

From **Fact 5**, since (ab) x" + m y" = 1 we conclude that gcd(ab,m) = 1.

Fact 7: For any integer I, gcd(a + Im, m) = gcd(a,m). (G.10)

Proof: (1) Let s be some common divisor of a and m. Clearly s divides a+Im. Thus, s is a common divisor of the pair a+Im and m. So

{ common divisors of a and m } $\subset$ { common divisors of a+Im and m } . (*)

(2) Let s be some common divisor of a+Im and m. Does s divide a? To find out, consider

$a+Im = s\,N_1$
$m = s\,N_2$

$$N_1 = \frac{a+Im}{s} = \frac{a}{s} + I\frac{m}{s} = \frac{a}{s} + I\,N_2 \quad \Rightarrow \quad \frac{a}{s} = N_1 - I\,N_2$$

Thus, $\frac{a}{s}$ is an integer so yes, s does divide a. Thus, s is a common divisor of m and a. So

{ common divisors of a+Im and m } $\subset$ { common divisors of a and m } (**)

(3) We conclude from (*) and (**) that the two common divisor sets are the same set, call it Q. Suppose this set is Q = {1, 5, 17}. Then gcd(a + Im, m) = 17 and gcd(a,m) = 17. In general, we find that both gcd(a + Im, m) and gcd(a,m) will be the largest element of Q, so gcd(a + Im, m) = gcd(a,m). QED.

Fact 8: gcd(a mod m, m) = gcd(a,m) (G.11)

Proof: We know that a mod m = a + Im for some integer I (I < 0 if a > m). Thus from **Fact 7** we have that gcd(a mod m, m) = gcd(a + Im, m) = gcd(a,m). QED

Fact 9: For a,b in Z_m (with + and •), gcd(a•b, m) = gcd(ab mod m, m) = gcd(ab,m). (G.12)

Proof: The meaning of a•b is that this product is some element c within Z_m which is closed under •. The rule for finding this element c is c = ab mod m, so a•b = ab mod m. Then the last equality shown follows from **Fact 8**.

Definition: Integers n and m are **coprime** (relatively prime) iff GCD(n,m) = 1. (G.13)

Definition: The set of integers < n which are coprime with n are called the **totatives** of n.
We shall refer to this set as G_n in what follows. (G.14)

Example: The totatives of n = 12 are {1,5,7,11} .

Definition: **Euler's totient function** φ(n) is the number of totatives of n. (G.15)

Examples: φ(12) = 4 since the set {1,5,7,11} has four elements.
φ(7) = 6 since the set {1,2,3,4,5,6} has 6 elements.
φ(p) = p-1 if p is prime

Comment: It happens that the sum of the totatives of n is (n/2)φ(n), but we shall not prove it since we don't need it. In our example with n = 12, 1+5+7+11 = 24 and (n/2)φ(n) = 6*φ(12) = 6*4 = 24.

Here are the first 100 values of φ(n) in the form

Fact 10: The set G_n of the totatives of n forms an abelian group under • within Z_n of order φ(n). (G.16)

Proof: The properties of a group are shown in (1.1). We know that G is closed under • from **Fact 6** which reads " if a and b are in G_n, then ab is in G_n ". We know from **(1.29)** that Z_n forms an abelian ring with

identity, so any subset of Z_n which includes 1 has the commutative, associative, and identity-exists properties for operator •. What is missing is the existence of a • inverse. When n is a prime p, we showed such an inverse always exists and Z_p is then a field GF(p). But for general Z_n some inverses do not exist. However, for our set G_n inverses always exist due to **Corollary 4** above. Thus G_n is a group of order φ(n).

Example: $Z_8 = \{0,1,2,3,4,5,6,7\} = Mod(8,+,\bullet)$

$G_8 = \{1,3,5,7\}$ with • operation of Z_8. Note that φ(8) = 4.

$3 \bullet 3 = 9 \bmod 8 = 1 \in G_8$ $\quad 3^{-1} = 1$ $\quad 5 \bullet 5 = 15 \bmod 8 = 7 \in G_8$ $\quad 5^{-1} = 7$

$3 \bullet 5 = 15 \bmod 8 = 7 \in G_8$ $\quad 5 \bullet 7 = 35 \bmod 8 = 3 \in G_8$

$3 \bullet 7 = 21 \bmod 8 = 3 \in G_8$ $\quad 7 \bullet 7 = 49 \bmod 8 = 1 \in G_8$ $\quad 7^{-1} = 1$

Thus, G_8 is closed under • and all elements have an inverse.

Fact 11: (Euler's Theorem). For any a in G_n, $a^{\varphi(n)} = 1 \bmod n$. (G.17)

Proof: **Fact (1.9e)** says that for any a in group G, $a^n = 1$ where n is the order of the group. What that means here is a•a•a...•a = 1 where we have φ(n) factors of a since from **Fact 10** the order of G_n is φ(n). The operation • is that of Z_n of which G_n is a subset. For elements in Z_n we know that a•b= ab mod n. Thus, a•a•a...•a $= a^{\varphi(n)} \bmod n$ if we interpret $a^{\varphi(n)}$ as aaaa..a (integer multiplication). Thus, we have Euler's Theorem:

$a \bullet a \bullet a ... \bullet a = a^{\varphi(n)} \bmod n = 1$ or $a^{\varphi(n)} = 1 \bmod n$ // see (G.3)

This theorem was proved by Euler in 1763. The theorem and the totient function φ(n) play a major role in current day RSA public key cryptography.

Fact 12: (Fermat's Little Theorem). If p is prime and a is any integer, then $a^p = a \bmod p$. (G.18)

Proof: For n = prime p, $G_p = \{1,2,3, ... p-1\} = Z_p$ and φ(p) = p-1. **Fact 11** then says $a^{p-1} = 1 \bmod p$ for any a in G_p. Since any a in G_p and p are coprime, meaning GCD(a,p) =1, we can apply **Corollary 3** and multiply both sides of $a^{p-1} = 1 \bmod p$ by a to get $a^p = a \bmod p$ for any a in $G_p = Z_p$. We can then extend the theorem to any integer a using **Fact 0** to say,

$a^p \bmod p = \{[a \bmod p] * [a \bmod p] ...\} \bmod p = [a \bmod p]^p \bmod p = 1$

where the last equality follows since a mod p lies in G_p. There is no restriction to positive integers, since every negative integer is congruent to a positive integer, such as (-19) mod 7 = (-5) mod 7 = 2 mod 7 = 2. Then $[(-19)^7 - (-19)] \bmod 7 = (2^7 - 2) \bmod 7 = 126 \bmod 7 = 0$. Also, for a = 0, $0^p = 0 = 0 \bmod p = 0$.

Comments: This theorem was stated by Fermat in 1640 without proof (as was his custom) and was later proved by Euler in 1736. In the Fermat primality test, if one can find an integer a such that $a^{p-1} \bmod p \neq 1$, one knows that p is not prime. The converse of the theorem is not true: that $a^p = a \bmod p$ for all a => p is prime. This converse fails for integers known as Carmichael numbers (Fermat pseudoprimes), the smallest of which is 561 (found in 1910 by Carmichael). Here we test 561 = 3*11*17 for a = the first 10,000 integers:

```
p := 561: ifactor(561);
                                                    (3) (11) (17)
found := false:
for a from 1 to 10000 do
  if (a^p-a) mod p <> 0 then print(a);found := true; fi;
od;
if found = false then print("no exceptions found"); fi;
                                                    "no exceptions found"
```

There are an infinite number of these pseudoprimes.

Fermat's "big" theorem was his Last Theorem which says that the Diophantine equation $x^n + y^n = z^n$ has no solutions for n > 2 and x,y,x > 0. This theorem was conjectured by Fermat in 1637 in a margin note and was first proved by Andrew Wiles in 1995, some 358 years after the conjecture was made.

Fact 13: The number of primitive elements in Galois Field GF(q=p^m) is φ(p^m-1). (G.19)

Proof: First we quote (4.32):

Fact 12: A power α^k of a known primitive element α of GF(q) is itself a primitive element if and only if GCD(k,q-1) = 1. *(4.32)*

Since powers of α enumerate all of {GF(q) - 0, • }, we can just try all powers α^k for k = 1 to q-2 and see whether or not the condition GCD(k,q-1) = 1 is valid for that power. If the condition is true, α^k is a primitive element. Then the number of primitive elements of GF(q) is the number of integers k < q-1 which are coprime to q-1. But this is exactly the set G_{q-1} of totatives of q-1 discussed above, a set we showed has φ(q-1) elements. Thus, the number of primitive elements of GF(q) is just φ(q-1). QED

Fact 14: The number of primitive polynomials in Galois Field GF(p^m) is φ(p^m -1)/m. (G.20)

Proof: We know from (5.15) that a primitive polynomial has coefficients which lie in a conjugate set which contains m elements, all of which are primitive elements. The primitive polynomials for all m elements in such a conjugate set are the same primitive polynomial since they have the same roots of GF(q). Thus, we have to divide the total count of primitive elements by m to get the total number of distinct primitive polynomials for GF(q). QED.
