Number Theory Homework.

1. The Theorems of Fermat, Euler, and Wilson.

1.1. **Fermat's Theorem.** The following is a special case of a result we have seen earlier, but as it will come up several times in this section, we repeat it here.

Proposition 1. *Let p be a prime and let a be an integer such that $p \nmid a$. Then*

$$ax \equiv ay \mod p \qquad \Longrightarrow \qquad x \equiv y.$$

Proof. If $ax \equiv ay \mod p$, then $p \mid a(y-x)$. As p is prime this implies $p \mid a$ or $p \mid (y-x)$. But $\nmid a$ and therefore $p \mid (y-x)$ which implies $x \equiv y \mod p$. □

Proposition 2. *If p is prime, then $p \nmid (p-1)!$.*

Problem 1. Prove this. □

Problem 2. It is important that p is prime in the last result. Give an example where n is positive and composite and $n \mid (n-1)!$. More generally Show that if $n \geq 6$ and n is composite, then $n \mid (n-1)!$. □

The following is anther result we have seen before.

Proposition 3. *If p is prime and $p \nmid a$, then after maybe reordering, the list of residue classes of*

$$a, 2a, 3a, \dots, (p-1)a$$

is the same as the list of residue classes of

$$1, 2, 3, \dots, (p-1).$$

More explicitly we can reorder the set $\{1, 2, 3, \dots, (p-1)\}$ as $r_1, r_2, r_3, \dots, r_{p-1}$ in such a way that

$$a \equiv r_1 \mod p, \quad 2a \equiv r_2 \mod p, \quad \dots \quad (p-1)a \equiv r_{p-1} \mod p.$$

Proof. Let $1 \leq j \leq (p-1)$. Then $p \nmid j$ and by assumption $p \nmid a$. Therefore $p \nmid ja$. Using the division to divide p into ja we get

$$ja = q_j p + r_j \qquad \text{where} \qquad 1 \leq r_j \leq (p-1).$$

(The reason that $r_j \neq 0$ is that p does not divide ja and therefore the remainder is not 0.) Then

$$ja \equiv r_j \mod p$$

If $r_i = r_j$, then $ia \equiv r_i = r_j \equiv ja \mod p$. That is $aj \equiv ai \mod p$. By Proposition 1 this implies $i \equiv j \mod p$. But $1 \leq i, j \leq (p-1)$ and therefore $i \equiv j \mod p$ implies $i = j$. Thus $r_i = r_j$ implies $i = j$. This implies that $r_1, r_2, \dots, r_{p-1}$ is a list of the $(p-1)$ distinct elements of $\{1, 2, \dots, (p-1)\}$ a set of size $(p-1)$. Therefore the set $r_1, r_2, \dots, r_{p-1}$ is a list of the elements of the set $\{1, 2, \ldots, (p-1)\}$ where each element appears exactly once in the list. $\square$

Let us look at an example related to these ideas. Let $p = 11$ and $a = 4$. Then Proposition 3 gives that

$$1 \cdot 4,\ 2 \cdot 4,\ 3 \cdot 4,\ 4 \cdot 4,\ 5 \cdot 4,\ 6 \cdot 4,\ 7 \cdot 4,\ 8 \cdot 4,\ 9 \cdot 4,\ 10 \cdot 4$$

are congruent mod 11 to to the elements of the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ in some order. And we can be specific

$$\begin{array}{lllll} 1 \cdot 4 \equiv 4, & 2 \cdot 4 \equiv 8, & 3 \cdot 4 \equiv 1, & 4 \cdot 4 \equiv 5, & 5 \cdot 4 \equiv 9, \\ 6 \cdot 4 \equiv 2, & 7 \cdot 4 \equiv 6, & 8 \cdot 4 \equiv 10, & 9 \cdot 4 \equiv 3, & 10 \cdot 4 \equiv 7, \end{array}$$

where all the congruences are $\pmod{11}$. Now someone clever, mostly likely Fermat or Euler, had the idea of multiplying these all together to get

$$\begin{aligned} &(1 \cdot 4)(2 \cdot 4)(3 \cdot 4)(4 \cdot 4)(5 \cdot 4)(6 \cdot 4)(7 \cdot 4)(8 \cdot 4)(9 \cdot 4)(10 \cdot 4) \\ &\qquad \equiv 4 \cdot 8 \cdot 1 \cdot 5 \cdot 9 \cdot 2 \cdot 6 \cdot 10 \cdot 3 \cdot 7 \pmod{11} \end{aligned}$$

By changing the order in the product we see

$$4 \cdot 8 \cdot 1 \cdot 5 \cdot 9 \cdot 2 \cdot 6 \cdot 10 \cdot 3 \cdot 7 = 10!.$$

Also

$$(1 \cdot 4)(2 \cdot 4)(3 \cdot 4)(4 \cdot 4)(5 \cdot 4)(6 \cdot 4)(7 \cdot 4)(8 \cdot 4)(9 \cdot 4)(10 \cdot 4) = 10!\, 4^{10}$$

Combining these gives

$$10!\, 4^{10} \equiv 10! \pmod{11}.$$

But $11 \nmid 10!$ and therefore by Proposition 1 we can cancel the $10!$ to conclude

$$4^{10} \equiv 1 \pmod{11}.$$

There was nothing special about the prime 11 or the number 4 in this. Let us do anther example, this time with $p = 7$ and a any integer with $7 \nmid a$. Then by Proposition 3 the numbers

$$a,\ 2a,\ 3a,\ 4a,\ 5a,\ 6a$$

are $\equiv \pmod 7$ to the numbers

$$1,\ 2,\ 3,\ 4,\ 5,\ 6$$

in some order. As the order of numbers in a product does not matter we thus have

$$(a)(2a)(3a)(4a)(5a)(6a) \equiv (1)(2)(3)(4)(5)(6) \pmod 7$$

which implies

$$6!\, a^6 \equiv 6! \pmod 7.$$

As $7 \nmid 6!$ we can cancel the $6!$ to get

$$a^6 \equiv 1 \pmod 7$$

for all integers a such that $7 \nmid a$.

At this point you may have already conjectured the following:

Theorem 4 (Fermat's little Theorem)**.** *Let p be a prime and a an integer with $p \nmid a$. Then*

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

Problem 3. Prove this. *Hint:* Here is an argument motivated by the examples above. Let $r_1, r_2, \ldots, r_{p-1}$ be as in Proposition 3. In particular this means that $r_1, r_2, \ldots, r_{p-1}$ a listing of the set $\{1, 2, \ldots, (p-1)\}$ and

$$a \equiv r_1 \mod p, \quad 2a \equiv r_2 \mod p, \quad \ldots \quad (p-1)a \equiv r_{p-1} \mod p.$$

These can be multiplied to get

$$a(2a)(3a)\cdots((p-1)a) \equiv r_1 r_2 r_3 \cdots r_{p-1} \mod p.$$

(a) Explain why

$$r_1 r_2 r_3 \cdots r_{p-1} = (p-1)!.$$

(b) Show

$$a(2a)(3a)\cdots((p-1)a) = (p-1)!\, a^{p-1}.$$

(c) Put these pieces together to conclude

$$(p-1)!\, a^{p-1} \equiv (p-1)! \mod p$$

Now you should be able to use Propositions 1 and 2 to finish the proof. □

Fermat's theorem is often stated in a slightly different form:

Theorem 5 (Fermat's little Theorem)**.** *If p is a prime, then for any integer a*

$$a^p \equiv a \mod p.$$

Problem 4. Prove this. *Hint:* We are trying to show $a^p - a = a(a^{p-1} - 1) \equiv 0 \mod p$. Now consider two cases $p \mid a$ (so that $a \equiv 0 \mod p$) and $p \nmid a$ (where the first form of Fermat's Theorem applies). □

Example 6. What is the remainder when 16^{205} is divided by 23? From Fermat's Little Theorem we know

$$16^{22} \equiv 1 \mod 23.$$

If we divide 22 into 205 the result is

$$205 = 9(22) + 7.$$

Therefore

$$16^{205} = 16^{9(22)+7} = \left(16^{22}\right)^9 (16)^7 = (1)^9 (16)^7 = 16^7.$$

Now

$$16^2 = 256 \equiv 3 \mod 23, \qquad 16^4 = (16^2)^2 \equiv 3^2 \equiv 9 \mod 23.$$

Thus

$$16^{205} \equiv 16^7 \equiv 16 \cdot 16^2 \cdot 16^4 \equiv 16 \cdot 3 \cdot 9 \equiv 16 \cdot 4 \equiv 18 \mod 23$$

where at one step we used $3 \cdot 9 = 27 \equiv 4 \mod 23$. Thus the remainder when 16^{205} is divided by 23 is 18. □

Problem 5. Compute the following: (a) The remainder when 10^{45} is divided by 13. (b) The remainder when 605^{67} is divided by 7 (for this you may want to start by noting $605 \equiv 3 \mod 7$). (c) The remainder when 23^{307} is divided by 31. □

Example 7. Find the remainder when 7^{23} is divided by 15. Here Fermat's Theorem does not apply directly, but the Chinese Remainder Theorem can help us out. Noting $15 = 3 \cdot 5$. Let us find the remainder when 7^{23} is divided by 3. In this case this is almost too easy:

$$7^{23} \equiv 1^{23} \equiv 1 \mod 3.$$

Now we have $7^{23} \equiv 2^{23} \mod 5$ and by Fermat's Theorem $2^4 \equiv 1 \mod 5$. Thus

$$7^{23} \equiv 2^{23} \equiv (2^4)^5(2)^3 \equiv 1^5 2^3 \equiv 8 \equiv 3 \mod 5.$$

Therefore 7^{23} is a solution to the the Chinese Remainder Problem

$$\begin{aligned} x &\equiv 1 \mod 3 \\ x &\equiv 3 \mod 5. \end{aligned}$$

We solve this and find the least positive solution is $x = 13$. The solution to this Chinese Remainder Problem is unique modulo the product $3 \cdot 5 = 15$. Thus

$$7^{23} \equiv 13 \mod 15$$

and therefore the remainder when 7^{23} is divided by 15 is 13. □

Problem 6. Use the method of the last example to find the remainder when 9^{45} is divided by 21. □

Problem 7. Find the remainder when 6^{273} is divided by $5 \cdot 7 \cdot 11 = 385$ by finding the remainders when it is divided by 5, 7, and 11 and then using the Chinese Remainder Theorem. □

Here is a more interesting application of Fermat's Theorem.

Proposition 8. *Let p be a prime and a an integer with $p \nmid a$. Then $\widehat{a} := a^{p-2}$ is an inverse of a modulo p. That is*

$$\widehat{a}a \equiv 1 \mod p.$$

Problem 8. Prove this. *Hint:* $\widehat{a}a = a^{p-1}$. □

1.2. **Binomial coefficients and anther proof of Fermat's Theorem.** To motivate this recall the binomial theorem for $n = 3$:

$$(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3.$$

If we view this modulo 3 and use that $3 \equiv 0 \mod 3$ we find

$$(x + y)^3 \equiv x^3 + y^3 \mod 3$$

holds for all integers x and y. Now let a be an integer such that

$$a^3 \equiv a \mod 3.$$

Then

$$\begin{aligned}(a+1)^3 &\equiv a^3 + 1^3 && \mod 3 \\ &\equiv a+1 && \mod 3 \qquad (\text{Using } a^3 \equiv a \mod 3).\end{aligned}$$

Therefore we have that for any integer a

$$a^3 \equiv a \mod 3 \qquad \Longrightarrow \qquad (a+1)^3 \equiv (a+1) \mod 3$$

and we have a "base case" of $a = 0$:

$$0^3 \equiv 0 \mod 3.$$

Thus by induction we have that $a^3 \equiv a \mod 3$ for all $a \geq 0$. If $a < 0$ then $b = -a > 0$ and so $b^3 \equiv b \mod 3$. Thus

$$a^3 \equiv (-b)^3 \equiv -b^3 \equiv -b \equiv a \mod 3$$

and it follows that $a^3 \equiv a$ for all integers a.

Next consider

$$(x+y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5.$$

The coefficients of all but the first and last term are divisible by 5 which implies

$$(x+y)^5 \equiv x^5 + y^5 \mod 5.$$

Therefore we can do similar inductive proof to show that $a^5 \equiv a \mod 5$ for all a.

As one more example

$$(x+y)^7 = x^7 + 7x^6y + 21x^5y^2 + 35x^4y^3 + 35x^3y^4 + 21x^2y^5 + 7xy^6 + y^7$$

and again all the coefficients other than the first and last are divisible by 7 leading to

$$(x+y)^7 \equiv x^7 + y^7 \mod 7$$

for all integers x and y.

So what we would like to be true is

Proposition 9. *Let p be a prime and $1 \leq k \leq p-1$. Then the binomial coefficient $\binom{p}{k}$ is divisible by p. That is*

$$\binom{p}{k} \equiv 0 \mod p \qquad \textit{for} \qquad 1 \leq k \leq p.$$

Lemma 10. *If p is a prime and $k < p$ then $p \nmid k!$.*

Problem 9. Prove this. *Hint:* Towards a contradiction assume that $p \mid k! = 1 \cdot 2 \cdot 3 \cdots k$. Then, as p is prime, p must divide one of the factors in this product. □

Proof of Proposition 9. Let p be prime and $1 \leq k \leq (p-1)$.

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}.$$

This implies

$$p! = k!(p-k)!\binom{p}{k}$$

and in particular that p divides $k!(p-k)!\binom{p}{k}$. As p is prime this implies

$$p \mid k!, \qquad p \mid (p-k)!, \qquad \text{or} \qquad p \mid \binom{p}{k}.$$

But $k < p$ so by that last lemma $p \nmid k!$. As $k \geq 1$ we have $(p-k) < p$ so the last lemma again applies and $p \nmid (n-k)!$. This only leaves $p \mid \binom{p}{k}$. □

Proposition 11. *If p is prime then for any integers x and y*

$$(x+y)^p \equiv x^p + y^p \mod p.$$

More generally for any integers $x_1, x_2, \ldots, x_m$ the congruence

$$(x_1 + x_2 + \cdots + x_m)^p = x_1^p + x_2^p + \cdots + x_n^p$$

holds.

Problem 10. Prove this. *Hint:* To prove the first congruence start with

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{n-k} y^k$$

and use $\binom{p}{k} \equiv 0 \mod p$ for $k = 1, 2, \ldots, p-1$ to see that when this is viewed mod p all but the first and last terms vanish. The second congruence follows form the first by an easy induction. □

Problem 11. Use the last proposition to show for any prime for any prime p and any integer a

$$a^p \equiv a \mod p \qquad \Longrightarrow \qquad (a+1)^p \equiv (a+1) \mod p$$

and use this to give an induction proof of Fermat's Theorem that $a^p \equiv a \mod p$. *Hint:* This can be done along the lines of the proof we gave in the case of $p = 3$ above. □

Problem 12. Here is another way to prove Fermat's theorem, although it is closely related to proof in the last problem. Let p be a prime. Then by Proposition 11 we have for any integers $x_1, x_2, , \ldots, x_n$ that

$$(x_1 + x_2 + \cdots + x_n)^p \equiv x_1^p + x_2^p + \cdots + x_n^p \mod p.$$

If a is a positive integer let $n = a$ and $x_1 = x_2 = \cdots = x_n = 1$. Then this congruence becomes

$$(\underbrace{1 + 1 + \cdots + 1}_{a \text{ terms in the sum}})^p \equiv \underbrace{1^p + 1^p + \cdots + 1^p}_{a \text{ terms in the sum}} \mod p$$

and you should be able to reduce this to $a^p \equiv a \mod p$. Now show it also holds for negative a. □

Problem 13. Show that the following identities do *not* hold.

$$\begin{aligned}(x+y)^4 &\equiv x^4 + y^4 \mod 4\\ (x+y)^6 &\equiv x^6 + y^6 \mod 6\\ (x+y)^8 &\equiv x^8 + y^8 \mod 8\\ (x+y)^9 &\equiv x^9 + y^9 \mod 9.\end{aligned}$$

□

Recreational Extra Credit Problem. Show that if $n \geq 2$ is an integer such that

$$(x+y)^n \equiv x^n + y^n \mod n$$

for all integers x and y, then n is a prime number. □

1.3. **Euler's Theorem.** Euler's theorem is a generalization of Fermat's theorem to moduli that are not prime. Our first proof of Fermat's theorem was to take a prime p and a number a with a with $\gcd(a,p) = 1$ and note that $1, 2, 3, \ldots, (p-1)a$ and $a, 2a, 2a, \ldots, (p-1)a$ when viewed modulo p were just rearrangements taking the products of these two sets of numbers would be congruent mod p which leads to $(p-1)! \equiv (p-1)!\, a^{n-1}$ and $\gcd(p, (p-1)!) = 1$ so that we can cancel to get $1 \equiv a^{p-1} \mod p$.

We can try the same thing with a composite n. If $\gcd(a,n) = 1$, then it will still be the case that $a, 2a, 3a, \ldots, (n-1)a$ when viewed mod n will be a rearrangement of $1, 2, 3, \ldots, (n-1)$ and so the products of the elements of the two lists will be congruent modulo n which leads to

$$(n-1)!a^{n-1} \equiv (a)(2a)\cdots((n-1)a) \equiv (1)(2)\cdots(n-1)! \mod n.$$

But if n is not prime we no longer have $\gcd(n, (n-1)!) = 0$. In fact

Problem 14. Show that if $n \geq 5$ is composite then $n \mid (n-1)!$. Thus 4

But if $n \mid (n-1)!$ the congruence $(n-1)!a^{n-1} \equiv (n-1)!$ reduces to $0 \equiv 0 \mod n$, which is true but not very interesting.

To get an interesting result we need to get a product of numbers that is relatively prime to n so that we can cancel. This suggests introducing the set following numbers.

$$U(n) := \{k : 1 \leq k \leq n \text{ and } \gcd(k,n) = 1\}.$$

(We are using the notation $U(n)$ because a number k has an inverse modulo n if and only if $\gcd(a,k) = 1$. Thus the residue classes of elements $U(n)$ are the elements of $\mathbb{Z}/p$ that have inverses. In ring theory elements with inverses are called units.) The following function will be important in much of what follows.

Definition 12. If n is a positive integer then the ***Euler phi function*** (or just the ***phi function***) is

$$\phi(n) = \#U(n) = \text{number of elements in } U(n).$$

□

Here are $\phi(n)$ and $U(n)$ for some small values of n.

n	$\phi(n)$	$U(n)$
1	1	{1}
2	1	{1}
3	2	{1, 2}
4	2	{1, 3}
5	4	{1, 2, 3, 4}
6	2	{1, 5}
7	6	{1, 2, 3, 4, 5, 6}
8	4	{1, 3, 5, 7}
9	6	{1, 2, 4, 5, 7, 8}
10	4	{1, 3, 7, 9}
11	10	{1, 2, 3, 4, 5, 6, 7, 8, 9, 10}
12	4	{1, 5, 7, 11}
13	12	{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12}
14	6	{1, 3, 5, 9, 11, 13}
15	8	{1, 2, 4, 7, 8, 11, 13, 14}
16	8	{1, 3, 5, 7, 9, 11, 13, 15}
17	16	{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16}
18	6	{1, 5, 7, 11, 13, 17}
19	18	{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18}
20	8	{1, 3, 7, 9, 11, 13, 17, 19}
21	12	{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20}
22	10	{1, 3, 5, 7, 9, 13, 15, 17, 19, 21}
23	22	{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22}
24	8	{1, 5, 7, 11, 13, 17, 19, 23}
25	20	{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24}
26	12	{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25}
27	18	{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26}
28	12	{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27}

If p is a prime then $\gcd(p, k) = 1$ for $k = 1, 2, 3, \ldots, (p-1)$. Thus

Proposition 13. *If p is prime, then $\phi(p) = p - 1$ and $U(p) = \{1, 2, \ldots, p-1\}$.* □

Now back to generalizing Fermat's theorem. To start

Proposition 14. *Let $n \geq 2$ be a positive integer and a an integer with $\gcd(a, n) = 1$. Then when reduced modulo n the set*

$$aU(n) := \{ak : k \in U(n)\}$$

is a rearrangement of $U(n)$. That is if $U(n) = \{k_1, k_2, \ldots, k_{\phi(n)}\}$, then when the elements of the set $aU = \{ak_1, ak_2, \ldots, ak_{\phi(n)}\}$ are reduced $\bmod n$, they are a rearrangement if $\{k_1, k_2, \ldots, k_{\phi(n)}\}$.

Problem 15. Prove this. *Hint:* If $ak_1, ak_2 \in aU(n)$ and $ak_1 \equiv ak_2 \mod n$, then, and $\gcd(a,n) - 1$ we can cancel the a to get $k_1 \equiv k_2$. As $1 \leq k_1, k_2 \neq n$ this implies $k_1 = k_2$. Thus $aU(n)$ and $U(n)$ have the same number of elements Also if $ak \in aU(n)$, then then the least positive residue of ak, call it b, will satisfy $0 \leq b \leq n-1$ and $\gcd(n,b) = 1$. Therefore $b \in U(n)$. Thus when the elements of $aU(n)$ are reduces modulo n the result is in $U(n)$. Put these facts together to get that the reductions of $aU(n)$ are just the elements of $U(n)$. □

And here is the generalization of Theorem 4.

Theorem 15 (Euler's Theorem)**.** *Let n be a positive integer and a an integer with* $\gcd(a,n) = 1$. *Then*

$$a^{\phi(n)} \equiv 1 \mod n.$$

Problem 16. Prove this. *Hint:* This clearly holds for $n = 1$ so we assume $n \geq 2$. Let

$$U(n) = \{k_1, k_2, \dots, k_{\phi(n)}\}.$$

Then, with the notation of Proposition 14,

$$aU(n) = \{ak_1, ak_2, \dots, ak_{\phi(n)}\}$$

and by Proposition 14 when the numbers $ak_1, ak_2, \dots, ak_{\phi(n)}$ are reduced modulo n the result is a rearrangement of $k_1, k_2, \dots, k_{\phi(n)}$. Therefore the products of the numbers in these two lists will be congruent modulo n, that is

$$(ak_1)(ak_2)\cdots(ak_{\phi(n)}) \equiv (k_1)(k_2)\cdots(k_{\phi(n)}) \mod n$$

and therefore

$$k_1 \cdot k_2 \cdots k_{\phi(n)} a^{\phi(n)} \equiv k_1 \cdot k_2 \cdots k_{\phi(n)} a^{\phi(n)} \mod n.$$

Now explain why we can cancel $k_1 \cdot k_2 \cdots k_{\phi(n)}$ from the congruence to finish the proof. □

We have seen that $\phi(p) = p - 1$ when p is prime. We now compute $\phi(p^k)$ for p prime.

Proposition 16. *If p is prime and k is a positive integer, then*

$$\phi(p^k) = p^k - p^{k-1}.$$

Problem 17. Prove this. *Hint:* Let $a \in \{1, 2, \dots, p^k\}$. Then $a \notin U(p^k)$ if and only if $p \mid a$. Use this fact to show that the set of elements of $\{1, 2, \dots, p^k\}$ are not in $U(p^k)$ is $\{tp : 1 \leq t \leq p^{k-1}\}$. □

Proposition 17. *Let m and n be positive integers with* $\gcd(m,n) = 1$. *For each $a \in U(m)$ and $b \in U(n)$ let $f(a,b)$ be the unique solution to the Chinese remainder problem*

$$f(a,b) \equiv a \mod m$$
$$f(a,b) \equiv b \mod n.$$

with

$$1 \le f(a,b) < mn.$$

Then f is a one to one onto function between $U(m) \times U(n)$ and the set $U(mn)$. (Here $U(m) \times U(n) := \{(a,b) : a \in U(m), b \in U(n)\}$.) Therefore $U(m) \times U(n)$ and $U(mn)$ have the same number of elements.

To see what this means for the example where $m = 5$ and $n = 6$. Then $mn = 30$ and

$$\begin{aligned} U(5) &= \{1,2,3,4\} \\ U(6) &= \{1,5\} \\ U(30) &= \{1,7,11,13,17,19,23,29\} \end{aligned}$$

and $U(5) \times U(6)$ is the set of ordered pairs:

$$U(5) \times U(6) = \{(1,1),(1,5),(2,1),(2,5),(3,1),(3,5),(4,1),(4,5)\}.$$

To compute $f(1,1)$ we solve the Chinese remainder problem

$$f(1,1) \equiv 1 \mod 5, \qquad f(1,1) \equiv 1 \mod 6$$

which gives

$$f(1,1) = 1.$$

To find $f(3,5)$ we have to solve

$$f(3,5) \equiv 3 \mod 5, \qquad f(3,5) \equiv 5 \mod 6$$

which gives

$$f(3,5) = 23.$$

Here are the values of $f(a,b)$ for all values $(a,b) \in U(5) \times U(6)$:

$$\begin{array}{llll} f(1,1) = 1, & f(1,5) = 11, & f(2,1) = 7, & f(2,5) = 17, \\ f(3,1) = 13, & f(3,5) = 23, & f(4,1) = 19, & f(4,5) = 29, \end{array}$$

which does gives us all the values in $U(30)$ exactly once each. This is a case where the example is not very enlightening as to why the general case is true.

Lemma 18. *Let m and n be positive integers with $\gcd(m,n) = 1$ and a and b integers with*

$$\gcd(a,m) = \gcd(b,n) = 1.$$

Let c be an integer with

$$c \equiv a \mod m \qquad \textit{and} \qquad c \equiv b \mod n.$$

Then

$$\gcd(c, mn) = 1.$$

Problem 18. Prove this. *Hint:* Towards a contradiction, assume that $\gcd(c, mn) \neq 1$. Then there will be a prime p with $p \mid \gcd(c, mn)$. This implies $p \mid c$ and $p \mid mn$. As p is prime, we have $p \mid m$ or $p \mid n$. Without loss of generality we may assume $p \mid m$. Thus $p \mid \gcd(c, m)$. But, as $a \equiv c \mod m$, we have $\gcd(a, m) = \gcd(c, m)$. Now explain why this leads to a contradiction. □

Lemma 19. *Let m and n be positive integers and c an integer with $\gcd(c, mn) = 1$. If $a \equiv c \mod m$, show $\gcd(a, m) = 1$. (And so by symmetry if $b \equiv c \mod n$, then $\gcd(b, n) = 1$. You do not have to give a separate proof of this.)*

Problem 19. Prove this. □

Problem 20. Prove Proposition 17. *Hint:* Verify the following steps.

(a) If $(a, b) \in U(m) \times U(n)$ use Lemma 18 to show $\gcd(f(a, b), mn) = 1$ and therefore $f(a, b) \in U(mn)$.
(b) Use the uniqueness part of the Chinese Remainder Theorem to show f is one to one.
(c) Show f is onto. (If $c \in U(mn)$ then let a and b be such that $a \equiv c$ with $1 \leq a \leq m$ and let $b \equiv c \mod n$ with $1 \leq b \leq n$. Use 19 to show $a \in U(m)$ and $b \in U(n)$ explain why this shows f is onto.) □

Definition 20. Let f be a function from the positive integers $\mathbb{Z}_+ = \{1, 2, 3, \ldots\}$ to the real numbers. Then f is ***multiplicative*** iff for all positive integers m and n

$$\gcd(m, n) = 1 \qquad \Longrightarrow \qquad f(mn) = f(m)f(n).$$

Theorem 21. *The Euler ϕ function is multiplicative.*

Proof. This follows at once from the definition of ϕ and Proposition 17. □

A straightforward induction now yields:

Proposition 22. *Let $n_1, n)2, \ldots, n_k$ be positive integers with $\gcd(m_i, m_j) = 1$ for $i \neq j$. Then*

$$\phi(n_1 n_2 \cdots n_k) = \phi(n_1)\phi(n_2) \cdots \phi(n_k).$$

□

Problem 21. Give at least three examples of positive integers m and n such that $\phi(mn) \neq \phi(m)\phi(n)$. □

If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ with $p_1, p_2, \ldots, p_k$ distinct primes and each $\alpha_i \geq 1$ we have

$$\begin{aligned} \phi(n) &= \prod_{i=1}^{k} \phi(p_i^{\alpha_i}) \\ &= \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_1 - 1}). \end{aligned}$$

Thus

$$\phi(60) = \phi(2^2 \cdot 3 \cdot 5) = \phi(2^2)\phi(3)\phi(5) = (4-2)(2)(4) = 16.$$

A larger example:

$$\phi(113{,}400) = \phi(2^3{\cdot}3^4{\cdot}5^2{\cdot}7) = \phi(2^3)\phi(3^4)\phi(5^2)\phi(7) = (4)(54)(20)(6) = 25{,}920.$$

Problem 22. Show that it n is divisible by an odd prime, then $\phi(n)$ is even. □

Problem 23. Find all positive integers n such that $\phi(n)$ is odd. Prove that you have found them all. □

Problem 24. If n is odd, prove that $\phi(2n) = \phi(n)$. □

Proposition 23. *If n is a positive integer, then*

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

where the product is taken over all primes that divide p that divide n.

Problem 25. Prove this. *Hint:* As a start note that if p is a prime and k is a positive integer

$$\phi(p^k) = p^k - p^{k-1} = \left(1 - \frac{1}{p}\right) p^k.$$

□

As an example of the last Proposition note that the primes that divide $6! = 720$ are just the primes ≤ 6, that is 2, 3, and 5. Thus

$$\phi(720) = 720 \prod_{p|720} \left(1 - \frac{1}{p}\right) = 720 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 192.$$