Totient Function PhL 7.7.13

This is development material for Appendix G. I think all matters are resolved.

I am looking at this little Euler's Theorem proof

http://philosophyforprogrammers.blogspot.com/2011/07/clever-proof-of-eulers-theorem.html

> Euler's theorem: Suppose a, n are coprime. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.
>
> Note that, since $\phi(p) = p - 1$, this is just a generalization of Fermat's little theorem. Here's a three-step proof:
>
> 1. An integer a is invertible modulo n if and only if $gcd(a, n) = 1$ ("invertible" means there's some a^{-1} such that $aa^{-1} \equiv 1 \bmod n$). This is the Linear Congruence Theorem.
> 2. Consider the group G of all positive integers less than n which are invertible modulo n (formally, $G = (\mathbb{Z}/n\mathbb{Z})^{\times}$). $\phi(n)$ simply counts the number of positive integers a where $gcd(a, n) = 1$, so by (1) there are $\phi(n)$ elements in G (the order of G is $\phi(n)$). You can satisfy yourself that G follows the group axioms quickly.
> 3. Lagrange's theorem says that there must be some k such that $a^k = 1$ where k divides the order of the group, namely $\phi(n)$; let's say $km = \phi(n)$. Then $a^{\phi(n)} = a^{km} = (a^k)^m = 1^m = 1$ which proves our theorem!

1. Definition of the totient function φ(n).

So if you count the number of integers coprime to integer n which are less than n, you get φ(n).

First, lets verify this against my little table.

	coprimes to n	φ(n)
n = 1	1	1
n = 2	1	1
n=3	1,2	2
n=4	1,3	2
n = 5	1,2,3,4	4
n=6	1,5	2
n = 7	1,2,3,4,5,6	6

For prime number, φ(n) is always n-1.

2. Why is the number of primitive elements of GF(p^m) equal to φ(q-1) ?

We know that p^m-1 = q-1 which has a set of divisors which I know about, but I don't think that is the relevant item. Rather, recall this Fact

Fact 6: If β is any element of (α,n,•), then the order of β divides n, the order of α. More specifically, we claim that [order of β] = n/GCD(k,n) where $\beta = \alpha^k$. (4.21)

My corollary (stated in App E or F maybe). Let the group be (α,q-1,•) = {GF(q) - 0} so n = q-1. Here α is a primitive element of GF(q). Then the Fact says

[order of β] = (q-1)/GCD(k,q-1) where $\beta = \alpha^k$

A corollary to this would be

β = α^k is a primitive element if GCD(k,q-1) = 1 where k = 1,2...q-2 because $\alpha^{q-1} = 1$

Thus, for each k that is coprime to q-1 and is less than q-1, we get a primitive element which is different since all these powers are different. Thus

Number of primitive elements = number of integers k that are coprime to q-1 ≡ φ(n)

Wow, that was pretty easy.

3. If a and n are coprime, then there exists an inverse of a inside mod n

OK, let a be an element of mod(n). We seek an inverse b of a such that ab = 1.

OK, this leads to many details: Linear Congruence Theorem, and (a,b) notation for gcd(a,b).

One claim is this: (this is NOT in B&M except when (c,m) = 1.

Proposition: $ca \equiv cb \mod m$ is equivalent to $a \equiv b \mod \frac{m}{(c,m)}$.

http://math453spring2009.wikidot.com/lecture-7 is where I saw the above.

If I can prove this, then this proof of LCT makes sense:

Linear Congruences $ax \equiv b \mod m$

Theorem 1. *If $(a, m) = 1$, then the congruence $ax \equiv b \mod m$ phas exactly one solution modulo m.*

Constructive. Solve the linear system

$$sa + tm = 1.$$

Then

$$sba + tbm = b.$$

So

$$sba \equiv b \pmod{m}$$

gives the solution $x = sb$.

If u_1 and u_2 are solutions, then

$$\begin{aligned} & au_1 \equiv b \pmod{m} \text{ and } au_2 \equiv b \pmod{m} \\ \Longrightarrow\ & au_1 \equiv au_2 \pmod{m} \\ \Longrightarrow\ & u_1 \equiv u_2 \pmod{m} \quad \text{since } (a, m) = 1. \end{aligned}$$

So there is only one solution. □ □

and then I can apply this to the inverse idea and then to the group idea G and then get Euler's Theorem. This is definitely another Appendix if I want to do it. I have already made pretty good progress.

I am stuck now showing that (a,b) = (a+b,b). Proof supposedly in 3.6 of this book

Textbook:
Kenneth Rosen
Discrete Mathematics and Its Applications
Sixth Edition
McGraw Hill Publishing Company, 2007

Well, I got the book (parts missing) and found the proof. Here it is

LEMMA 1 Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

Proof: If we can show that the common divisors of a and b are the same as the common divisors of b and r, we will have shown that $\gcd(a, b) = \gcd(b, r)$, because both pairs must have the same *greatest* common divisor.

So suppose that d divides both a and b. Then it follows that d also divides $a - bq = r$ (from Theorem 1 of Section 3.4). Hence, any common divisor of a and b is also a common divisor of b and r.

Likewise, suppose that d divides both b and r. Then d also divides $bq + r = a$. Hence, any common divisor of b and r is also a common divisor of a and b.

Consequently, $\gcd(a, b) = \gcd(b, r)$. ◁

July 9, 2013. But found in my Euler's Theorem proof:

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:

$a•a•a...•a = a^{\varphi(n)} \bmod n = 1$ or $a^{\varphi(n)} = 1 \bmod n$

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.

I state the theorem only for a in G_n , but the real theorem says it is valid for all integers a. I have verified this in wiki. Hopefully I just have to modify things a bit. // I just added (1.31a,b) to formally state the mod arithmetic rules, I used these rules many times but never stated them!

Suppose b is some arbitrary integer. Then

$b^{\varphi(n)} \bmod n = (bbbb...b) \bmod n = [\, b \bmod n]^{\varphi(n)}$

so now at least we have b inside Z_n. If b mod n happens to be in G_n, then we know $[\, b \bmod n]^{\varphi(n)} = 1$. But suppose b is NOT in G_n. Then what happens? We know only that b is in Z_n. This ring is additively cyclic. Is it • cyclic as well? No, it is not a • cyclic group because it is not even a group since inverses are missing. Since Z_n is not a group, we cannot use any group theory theorem. Consider:

```
 with(numtheory):
arning, new definition for order
 n := 6: a := 4:
 f := (a^phi(n)-1) mod n;
```

$f := 3$

This shows that Euler's Theorem is NOT VALID for G_6 and a = 4. So OK, wiki and I both have this right.

Now look at Fermat. In this case p = 7 say, then
****

Example: $Z_8 = \{0,1,2,3,4,5,6,7\} = \text{Mod}(8,+,•)$
$G_8 = \{1,3,5,7\}$ with • operation of Z_8. Note that φ(8) = 4.
$3 • 3 = 9 \bmod 8 = 1 \in G_8$ $3^{-1} = 1$ $5 • 5 = 15 \bmod 8 = 7 \in G_8$ $5^{-1} = 7$
$3 • 5 = 15 \bmod 8 = 7 \in G_8$ $5 • 7 = 35 \bmod 8 = 3 \in G_8$

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

Thus, G_8 is closed under $\bullet$ and all elements have an inverse.

Hold this for a moment

In the above we may take $(\alpha,n,\bullet)$ to be $(\alpha,q-1,\bullet)$ where the cyclic group is *all* of {GF(q) - 0) }, as will be shown in Big Theorem 1 (4.30) below. The order this cyclic group is n = q-1. Thus, Fact 6 specialized to this case says [order of β] = (q-1)/GCD(k,q-1) where $\beta = \alpha^k$. Here α is an element of GF(q) which has order n=q-1 so that $\alpha^{q-1} = 1$. Such an element α is said to be a "primitive element", as described near (4.30) below. We have then proven this Corollary to Fact 6:

Corollary. If α is a primitive element of GF(q), and if GCD(k,q-1) = 1, then the element $\beta = \alpha^k$ is *also* a primitive element. this already appears as (4.32) below! (4.21a)