Finding a proof for the Divisor Theorem PhL 7.5.13

This all deals with what is now Fact 1 in Appendix E, so it is a done deal.

Fact 1: For any integer n not a multiple of prime p, one can find integer m such that n is a divisor of (p^m - 1). That is, we can find m such that (p^m-1) mod n = 0 which is the same as p^m mod n = 1. (E.1)

****

Here is my theorem:

Theorem: For any integer n not a multiple of p, you can find m such that n is a divisor of p^m - 1.

Maple is telling me this is true for any p. Maple suggests that the lowest solution value of m is ≤ n.

Here is someone who did exactly what I did on scratch paper at least for the first part:

Definition

What are the divisors of a number N? In general, the divisors of a number refer to the positive divisors, unless otherwise noted. Since the negative divisors will be the negative of a positive divisor (and vice versa), we shall just consider positive divisors.

Technique

Let the integer N have a prime factorization $p_1^{q_1} p_2^{q_2} \dots p_n^{q_n}$, where $p_1, p_2 \dots, p_n$ are distinct prime numbers, and $q_1, q_2 \dots q_n$ are positive integers. Let d be a divisor of N; then any prime factor p that divides d must divide N, hence it must be one of $p_1, p_2, \dots, p_n$.

Without loss of generality, set $p = p_i$. Let the highest power of p that divides d be $p_i^{r_i}$. Then, $p_i^{r_i}$ divides d, which in turn divides N, hence, $p_i^{r_i}$ must divide $p_i^{q_i}$, which means that $r_i \leq q_i$. Thus, by considering all the prime factors of d, we get that it must have the form $d = p_1^{r_1} p_2^{r_2} \dots p_n^{r_n}$ where $0 \leq r_i \leq q_i$ for all i.

Conversely, given a number d that has the form $d = p_1^{r_1} p_2^{r_2} \dots p_n^{r_n}$ where $0 \leq r_i \leq q_i$ for all i, it is clear that d is a divisor of N. As such, we have a complete classification of all the divisors.

Divisor Function

How many divisors does the number N have? From the above classification, we can set up a direct bijection between $d = p_1^{r_1} p_2^{r_2} \dots p_n^{r_n}$ and sets of n integers $(r_1, r_2, \dots r_n)$ that satisfy $0 \leq r_i \leq q_i$. For each r_i, there are $q_i - 0 + 1 = q_i + 1$ possibilities. Hence, by the product rule, there are going to be $(q_1 + 1)(q_2 + 1) \dots (q_n + 1)$ divisors in all. The number of divisors of an integer N is often denoted as the $\phi(N)$ or $\sigma_0(N)$.

So consider this simpler problem and maybe use it to find the proof. Imagine that we list of the prime numbers in order $p_1 = 1$, $p_2 = 2$, etc. Then suppose

$p = p_j$ for some j

$n = p_i$ for some $i \neq j$

See if you can find m that works for this simple case of n. We write

$p^m - 1 = \Pi_k p_k^{qk} = p_1^{q1} p_2^{q2} \dots$ Yes $p_1^{q1} = 1$ but I leave it there.

In particular, maybe I can find some p^m-1 of this form

$p^m - 1 = p_1^{q1} p_2^{q2} \dots p_i^1 \dots$ // there is no factor p_j^{qj} since $p^m - 1$ not multiple of p

Rewrite this as

$p_j^m - 1 = p_1^{q1} p_2^{q2} \dots p_i^1 \dots$ // no factor p_j^{qj}

Claim that we can find m to make this work. So what is it? All I care about is the p_i^1 factor so I will take take any m such that $p_j^m - 1$ has prime factor p_i. If these were true, then

$p_j^m - 1 = p_i N$ N = some integer with no factor p_i^k .

$p_j^m = p_i N + 1$

In fact ANY solution integer N would be fine by me. For example

$3^m = 5N + 1$

$5N = 3^m - 1$

$N = (3^m - 1)/5$ = integer

Consider f(m) = 3^m - 1 as a mapping from integers m to integers. How do we know that we will eventually land on an integer that is a multiple of 5 ? Simpler case

$N = (2^m - 1)/3$ = integer

How do we know that as we increase m, will eventually land on an integer that is a multiple of 3?

$2^1 - 1 = 1$
$2^2 - 1 = 3$ done.

Suppose there were no such m. Then we have

$(2^m - 1)/3 \neq$ integer for m = 1,2,3....∞

Need to know something about the "landing spots".

$a_m = 2^m - 1$
$a_{m+1} = 2^{m+1} - 1$

$a_{m+1} - a_m = 2^{m+1} - 1 - (2^m - 1) = 2^{m+1} - 2^m = 2^m(2-1) = 2^m$

This is the spacing between sequential landing spots. It is not a multiple of 3. Each step up in m causes us to move 2^m mod 3 on the grid. For m = 2, 2^m mod 3 = 1 so we moved on grid space to the right. So if we were short by 1, this fixes us up. If we were short by 2, then 2^4 mod 3 =

$a_m = 2^m - 1$
$a_{m+r} = 2^{m+r} - 1$

$a_{m+r} - a_m = 2^{m+r} - 1 - (2^m - 1) = 2^{m+r} - 2^m = 2^m(2^r - 1)$

Now we have freedom to select r. Suppose at m we are 2 short on the grid. Then we want to select r such that

$2^m(2^r - 1) \mod 3 = 2$

$(2^m \bmod 3) \otimes (2^r - 1) = 2$ inside GF(3)

Then

$(2^r - 1) = 2 \otimes (2^m \bmod 3)^{-1}$

I think that is it!

Now try a fancier case:

$p_j^m - 1 = p_i^2 N$ N = some integer with no factor p_i^k .

$p_j^m = p_i^2 N + 1$

In fact ANY solution integer N would be fine by me. For example

$3^m = 5^2N + 1$

$5^2N = 3^m - 1$

$N = (3^m - 1)/5^2$ = integer

$N = (2^m - 1)/3^2$ = integer

$a_{m+r} - a_m = 2^m(2^r-1)$

Suppose for some m I find that

$Rem[(2^m - 1)/3^2] = 2$

Then I want to increase m by r steps such that I move 7 grid spaces to the right. I want

$2^m(2^r-1) \bmod 9 = 7$

Mod(9) is GF(9) which is not a field so all elements don't have inverses.

I am back to square zero after an hour or two!

Maple shows that when I compute $Rem(p^m-1,n)$ for some fixed n and let m increase, the remainder sequences repeatedly through some sequence which always includes 0 but does not generally include all integers. This really can't be so complicated, can it?

Fact: If $Rem(p^m-1,n) = 0$, then $Rem(p^m,n)$

I first realized this from Little Lemma 2, but it is complete obvious of course. I now think this is true:

Theorem: Let p = prime < n. Then there exists integer k such that $p^k \bmod n = 1$.

This then is what makes the Maple repeating sequence.

Here is perhaps a lead from wiki on :
http://en.wikipedia.org/wiki/Multiplicative_group_of_integers_modulo_n

Powers of odd primes [edit]

For powers of odd primes p^k the group is cyclic:[2]

$$(\mathbb{Z}/p^k\mathbb{Z})^\times \cong \mathrm{C}_{p^{k-1}(p-1)} \cong \mathrm{C}_{\varphi(p^k)}.$$

But what is "the group" ? The notation above means Z / (p^k) but seems not too close to me.

Well, a red herring. This looks better in wiki

http://en.wikipedia.org/wiki/Fermat%27s_little_theorem

Generalizations [edit]

A slight generalization of the theorem, which immediately follows from it, is: if p is prime and m and n are *positive* integers such that $m \equiv n \pmod{p-1}$ then for every integer a we have $a^m \equiv a^n \pmod{p}$.

This follows as m is of the form $b(p-1)+n$, so $a^m = a^{b(p-1)} \cdot a^n \equiv 1^b \cdot a^n \equiv a^n \pmod{p}$.

In this form, the theorem is used to justify the RSA public key encryption method.[*citation needed*]

Fermat's little theorem is generalized by Euler's theorem: for any modulus n and any integer a coprime to n, we have

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

where $\varphi(n)$ denotes Euler's totient function (which counts the integers between 1 and n that are coprime to n). This is indeed a generalization, because if $n = p$ is a prime number, then $\varphi(p) = p - 1$.

This can be further generalized to Carmichael's theorem, as well as to Lagrange's theorem in group theory.

Fermat's little theorem also has a generalization in finite fields.

That Euler's Theorem thing has mod n for any n, which is what I am looking for. I know that

gcd(p, n) = 1 if n is my integer which is not a multiple of p which is prime

Thus, this Euler theorem would say for a = p

$p^{\varphi(n)} \bmod n = 1$

This then gives me the exponent k I have been looking for.

Example: n = 4, p = 3, I know that $p^2 = 9 = 1$. And $\varphi(4) = 2$, check! This is my baby. Now can I zero in on this little theorem? Wiki has a page just on it!

https://en.wikipedia.org/wiki/Euler%27s_theorem

Here is a short proof, but it will require work on my part

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

I am optimistic. Now that I have a theorem I can quote, let's finish off what I was doing and only come back here and play if there is time. So:

Candidate Material for a new Appendix E (fin 7.6.13)

Fact: For any integer n not a multiple of prime p, one can find m such that n is a divisor of $p^m - 1$.

Proof: Saying that n is a divisor of p^m-1 is the same as saying Rem[$(p^m-1)/n$] = 0. This in turn is the same as saying Rem[p^m/n] = 1. If this is not obvious, it follows from Little Lemma 2 *****. Restating one more time, our theorem is equivalent to claiming there exists integer m such that $p^m \bmod n = 1$. Since we have assumed n is not a multiple of p, and that p is a prime number, we know that GCD(p,n) = 1, so p and n are coprime. After all, p cannot divide n, and nothing smaller than p can divide p but 1. A certain Euler's Theorem claims that for any element of Mod(n) that is coprime to n (such as our p), there exists an integer k such that $a^k \bmod n = 1$. In our case, that says $p^k \bmod n = 1$. If we select m = k, then $p^m \bmod n = 1$ and therefore Rem[p^m/n] = 1 and therefore Rem[$(p^m-1)/n$] = 0 and therefore n is a divisor of $p^m - 1$ for this value of m. Our theorem merely claims that such an integer m exists. It happens, according to Euler's Theorem, that the integer m = k is none other than φ(n), Euler's totient function. Integer n can be larger than or smaller than p.

Verification: Here we check the above Fact for the first 20 prime numbers and all n < 1000:

```
primes := seq(ithprime(i),i=1..20);
```

primes := 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71

```
found := false:
for p in [primes] do
  for n from 1 to 1000 do
    if n mod p = 0 then next; fi;   #ignore n being multiple of p
    m := phi(n);
    r := p^m-1 mod n;
    if r <> 0 then found := true; print("exception found", p, m, n) ;fi;
  od;
od;
if found = false then print("no exceptions were found"); fi;
```

"no exceptions were found"

Fact: If integer D is a divisor of q -1, then GF(q) has at least one element of order D.

Proof: We know from (4.21) that [order(α^k)] = (q-1)/GCD(k,q-1) where α is any primitive element of GF(q) and k any positive integer. Since D is a divisor of q-1 we can write DM = q-1 where M is the other factor. M then also divides q-1. Setting k = M,

[order(α^M)] = (q-1)/GCD(M,q-1)

But GCD(M,q-1) = M. The reason is that M is a candidate GCD since it divides M and q-1, and no larger integer can divide M, so M is it. Thus we have shown that [order(α^M)] = (q-1)/M = D. Thus we have found an element of GF(q), namely α^M , which has order D, for any D among the divisors of (q-1).

Example: For GF(2^4) we have q-1 = 15 which has divisors 1,3,5 and 15. If α is a primitive element, then we know $\alpha^{15} = 1$ since such an element has order q-1.

D	1	3	5	15
M	15	5	3	1
$\beta^{order}=1$	$(\alpha^{15})^1= 1$	$(\alpha^5)^3= 1$	$(\alpha^3)^5= 1$	$(\alpha^1)^{15}= 1$
order β	1	3	5	15

Here an element β of GF(q) has been found for each divisor of q-1. For D = 1, β = 1 and $1^1 = 1$ so the identity always has an order to match D = 1. For D = 15 we just get the statement that α is a primitive element $\alpha^{15}= 1$. It is the interior columns that are important.

Fact: If integer D is a divisor of q -1, then GF(q) has at least one minimum polynomial of period D.

Proof: From the previous fact, we know that GF(p^m) has at least one element α of order D. This element has a minimum polynomial m(x) of the form (x-α)(other factors) . From (5.66) we know that the period of a minimum polynomial is the same as the order of the elements in its conjugate set (here including α), so since α has order D, there exists m(x) of period D.

Example: Recall this enumeration (6.21) of the minimum polynomials of GF(2^4), where we have added the two trivial minimum polynomials shown in (5.24) which are always present :

$p_1(x)$	$= (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)$	$= x^4 + x + 1$	10011	
$p_7(x)$	$= (x - \alpha^7)(x - \alpha^{14})(x - \alpha^{13})(x - \alpha^{11})$	$= x^4 + x^3 + 1$	11001	
$m_3(x)$	$= (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9)$	$= x^4 + x^3 + x^2 + x + 1$	11111	
$m_5(x)$	$= (x - \alpha^5)(x - \alpha^{10})$	$= x^2 + x + 1$	111	(6.21)
$m_0(x)$	$= (x - \alpha^0) = (x-1)$;			
m_{zero}	$= (x - 0) = x$;			

We shall now compute the period of each. First the polynomials are entered:

```
p1 := x^4+x+1:
p7 := x^4+x^3+1:
m3 := x^4+x^3+x^2+x+1:
m5 := x^2+x+1:
m0 := x-1:
mzero := x:
```

The following procedure scans n downward to find the period of polynomial f(x) :

```
period := proc(f,q,p) local per, n;
  per := infinity;
  for n from q by -1 to 1 do if Rem(x^n-1,f,x) mod p = 0 then per := n; fi; od;
  RETURN(per);
end:
```

And here are the resulting periods:

```
period(p1,15,2);
                        15
period(p7,15,2);
                        15
period(m3,15,2);
                         5
period(m5,15,2);
                         3
period(m0,15,2);
                         1
period(mzero,15,2);
                        ∞
```

As claimed in the Fact, there exists a minimum polynomial of period D for each D that divides p^m-1. The function x can never divide any $x^n- 1$ so the procedure sets period = ∞.

Fact: For any n not a multiple of p, there exists a g(x) which divides $x^n - 1$ and which can therefore be used to construct a cyclic code of length n.

Proof: To find a suitable g(x) with coefficients in GF(p), we search through extension fields GF(p^m) for m = 1,2,3 ... . We know from Fact X that, for any divisor D of $p^m- 1$, GF(p^m) has a minimum polynomial m(x) of period D, so that m(x) divides x^D-1. If we can find a value of m such that $p^m - 1$ has a divisor D=n then m(x) divides $x^n - 1$ and this m(x) is a viable g(x). But Fact Y says that we *can* find m such that n is a divisor of $p^m -1$, namely, m = φ(n). Thus, the field GF($p^{\varphi(n)}$) has a suitable minimum polynomial that can be used for g(x).

Corollary: For any n not a multiple of p one can construct a cyclic code of length n whose polynomials have coefficients in GF(p).

BUT, for p - 2 I think I showed that there is a g(x) of every degree less than n which divides x^n-1, so that seems to by much more general than my result above.