Number Theory Coursework

The result proved in this coursework has also been proved using the same method in the Lean theorem prover. This is available at `https://github.com/ChrisHughes24/numbertheory`

1 Preliminaries

For this proof one related theorem is required. For any $n \in \mathbb{N}_{\geq 0}$, let $v_p(n)$ be the maximum integer k such that p^k divides n. Then for any integers $n > 0$, and $k > 0$, $v_p\binom{n}{k} \geq v_p(n) - v_p(k)$.

A theorem by Legendre says that for any n, $v_p(n!) = \sum_{i=0}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$.

To compute a bound on $v_p\binom{n}{k}$, observe that

$$\begin{aligned} v_p\binom{n}{k} &= v_p(n!) - v_p(k!) - v_p((n-k)!) \\ &= \sum_{i=0}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{k}{p^i} \right\rfloor - \left\lfloor \frac{n-k}{p^i} \right\rfloor \end{aligned} \tag{1}$$

Observe that if p^i divides n but not k then the corresponding term in the sum is 1, so the sum is at least as big as the number of i that divide n but not k, which is $v_p(n) - v_p(k)$

2 Main proof

Lemma 1 *If m is even then $x + 1$ is a power of 2*

Consider congruences mod p when m is even, and p divides $x^m + 1$. Then p also divides $x + 1$

$$x^m + 1 \equiv (-1)^m + 1 \equiv 2 \bmod p \tag{2}$$

So $2 = 0 \bmod p$ and therefore $p = 2$ and $x + 1$ is a power of 2.

Lemma 2 *If m is even then $x^m + 1 \equiv 2 \bmod 4$*

This is because x must be odd, so x^m is an odd square, so x^m is 1 mod 4.

Lemma 3 *m is odd*

Assume m is even.

By Lemma 1, x^m+1 is a power of 2. But by Lemma 2 x^m+1 is 2 mod 4. 2 is the only power of 2 congruent to 2 mod 4. So $x^m+1=2$, but this contradicts $x>1$ and $m>1$. So m is odd.

Lemma 4 $x+1$ *divides* x^m+1

-1 is a root of the polynomial X^m+1 since m is odd. So by the factor theorem $x+1$ divides x^m+1.

The idea of the rest of the proof is to prove that $\frac{x^m+1}{x+1}$ divides m, and is therefore less than or equal to m, which puts bounds on x and m. The divisibility is proven by proving every prime power that dividies $\frac{x^m+1}{x+1}$ also divides m.

Lemma 5 *Let p be a prime and suppose p^r divides m. Let t be a positive integer. Let i be an integer at least 2. The p^{r+t+1} divides $\binom{m}{i}p^{ti}$*

If $p=2$ then since m is odd, $r=0$. So $p^{r+t+1}=p^{t+1}$ which divides p^{ti}.

Otherwise, we use the fact that $v_p\binom{m}{i} \geq v_p(m)-v_p(i)$.

First prove that $p^{ti-t}>i$. $p^{ti-t}=p^tp^{t(i-2)} \geq 3p^{t(i-2)} \geq p^{t(i-2)}+2 > t(i-2)+2 \geq i$, So p^{ti-t} does not divide i.

Therefore $v_p\binom{m}{i} > v_p(m)-(ti-t)$. So $v_p\left(\binom{m}{i}p^{ti}\right) \geq v_p(m)+t$.

Lemma 6 *If p is prime and p^t divides $x+1$, but p^{t+1} does not divide $x+1$ and p^{s+t} divides x^m+1, then p^s divides m.*

If $t=0$ then s must also be equal to zero, since any prime dividing x^m+1 also divides $x+1$.

First prove that p^r divides m, when $r \leq s$ by induction on r. We can assume t is positive.

The case $r=0$ is trivial.

Now assume p^r divides m and deduce p^{r+1} divides m, provided $r<s$.

Write $x=kp^t-1$ where p does not divide k.

Then $x^m+1=(kp^t-1)^m+1=mkp^t-\sum_{i=2}^m \binom{m}{i}(-k)^ip^{it}$.

Using Lemma 5, p^{r+t+1} divides the sum. It also divides x^m+1, so p^{r+t+1} must divide mkp^t, so p^{r+1} divides m.

Lemma 7 $\frac{x^m+1}{x+1} \leq m$

By Lemma 6, every prime power that divides $\frac{x^m+1}{x+1}$ also divides m, So $\frac{x^m+1}{x+1}$ divides m and is therefore less than or equal to m.

Lemma 8 *m=3*

Suppose for a contradiction that $m \geq 4$. Write $m = m' + 4$, where $m' \in \mathbb{N}_0$. Similarly write $x = x' + 2$.

Now show $(m' + 4)(x' + 2) + m' + 4 < (x' + 2)^{m'+4} + 1$.

$$\begin{aligned} &(m' + 4)(x' + 2) + x'(m' + 4) \\ &= (3m' + 12) + x'(m' + 4) \\ &< (3(x' + 2)^{m'} + 12(x' + 2)^{m'}) + x'((x' + 2)^{m'} + 4(x' + 2)^{m'}) \\ &\leq (x' + 2)^{m'+4} + 1 \end{aligned} \tag{3}$$

But by Lemma 7, $(m' + 4)(x' + 2) + m' + 4 \geq (x' + 2)^{m'+4} + 1$, so m cannot be greater than 3. m is odd and $m > 1$ so $m = 3$

Lemma 9 *x=2*

Suppose for a contradiction that $x \geq 3$. Write $x = x' = 3$ Then

$$\begin{aligned} &mx + m \\ &= 3x' + 12 \\ &< x'^3 + 9x'^2 + 27x' + 27 \\ &= x^m + 1 \end{aligned} \tag{4}$$

So $x < 3$, but $x > 1$, so $x = 2$.

Lemma 10 *The solutions are $x = 2$, $m = 3$ and $n \geq 2$*

Given $x = 2$ and $m = 3$ simple calculations verify that this is a solution if and only if $n \geq 2$.