Introduction to Number Theory HW1

Angus Joshi

January 26, 2024

Claim 1. *For* $n \in \mathbb{Z}_{>1}$, $x \in \mathbb{Z}$, $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + ... + 1)$.

Proof. Simply multiplying out,

$$\begin{aligned}(x-1)(x^{n-1} + x^{n-2} + ... + 1) &= x^n + x^{n-1} + ... + x - x^{n-1} - x^{n-2} - ... - 1 \\ &= x^n - 1.\end{aligned}$$

□

Claim 2. *For* $d, n \in \mathbb{Z}_{>1}$, *if* $d^n - 1$ *is prime then* $d = 2$.

Proof. Suppose $d^n - 1$ is prime and $d > 2$. Then by claim 1 $d^n - 1 = (d-1)(d^{n-1} + ... + 1)$. It follows that $(d-1)|d^n - 1$. Noting that $d - 1 > 1$ by supposition, this contradicts $d^n - 1$ being prime. I conclude $d \leq 2$, which combining with $d > 1$ gives $d = 2$. □

Claim 3. *If* $n = ab$ *for* $a, b \in \mathbb{Z}_{>1}$, *then* $2^n - 1$ *is composite.*

Proof. Suppose $n = ab$ for $a, b \in \mathbb{Z}_{>1}$. Then,

$$\begin{aligned}2^n - 1 &= 2^{ab} - 1 \\ &= (2^a)^b - 1.\end{aligned}$$

Since $a > 1$ I have $2^a > 2$. Applying the contrapositive of claim 2 I find $2^n - 1$ is not prime. □

Claim 4. *If* $2^n - 1$ *is prime then* n *is prime.*

Proof. Precisely the contrapositive of claim 3. □

Claim 5. *For* $n \in \mathbb{Z}_{>1}$ *odd,* $x \in \mathbb{Z}$, $x^n + 1 = (x+1)(x^{n-1} - x^{n-2} + ... + 1)$.

Proof. Again multiplying out,

$$\begin{aligned}(x+1)(x^{n-1} - x^{n-2} + ... + 1) &= x^n - x^{n-1} + x^{n-2} - ... + 1 \\ &\quad + x^{n-1} - x^{n-2} + ... + x \\ &= x^n + 1.\end{aligned}$$

Note that n odd was used to ensure the correct sign in the alternating sum. □

Claim 6. *For $n \in \mathbb{Z}_{\geq 1}$ if $2^n + 1$ is prime and n is odd, then $n = 1$.*

Proof. Suppose $n > 1$ is odd and $2^n + 1$ is prime. Then by claim 5,

$$(2^n + 1) = (2 + 1)(2^{n-1} - ... + 1).$$

So $3|2^n+1$. But this contradicts 2^n+1 being prime, from which I find $n = 1$. $\square$

Claim 7. *For $n \in \mathbb{Z}_{\geq 1}$ if 2^n+1 is prime then there is no odd $q > 1$ that divides n.*

Proof. Suppose an odd $q > 1$ divides n. That is, for some m $n = qm$. Then using essentially the same argument as claim 6,

$$\begin{aligned}(2^n + 1) &= 2^{mq} + 1\\ &= (2^m)^q + 1\\ &= (2^m + 1)((2^m)^{n-1} - ... + 1).\end{aligned}$$

It follows that $2^m + 1$ divides $2^n + 1$, which is a contradiction to primeness. $\square$

Claim 8. *For $n \in \mathbb{Z}_{\geq 1}$ if $2^n + 1$ is prime then $n = 2^m$ for some $m \in \mathbb{Z}_{\geq 0}$.*

Proof. From claim 7 I immediately find n has no odd factors. The only non-odd prime number is 2, so the unique prime factorisation of n must consist only of 2s, completing the proof. $\square$