HW4

Number Theory, Fall 2020, UTK

Gregory Croisdale

1.3

18. Prove that $(a^2, b^2) = c^2$ if $(a, b) = c$.

By the Fundamental Theorem of Arithmetic, a and b can be uniquely defined by a product of prime factors. We can write a and b as products of the same primes f_i raised to different exponents n_i, m_i as illustrated below:

$\Rightarrow a = f_1^{n_1} \cdot f_2^{n_2} \cdot \ldots f_r^{n_r}$ where $f_i, n_i, r \in \mathbb{Z}$ and $n_i \geq 0$ and

$\Rightarrow b = f_1^{m_1} \cdot f_2^{m_2} \cdot \ldots f_r^{m_r}$ where $m_i \in \mathbb{Z}$ and $m_i \geq 0$.

By the definition of the gcd, $gcd(a, b) = f_1^{k_1} \cdot f_2^{k_2} \cdot \ldots f_r^{k_r}$ where $k_i = \min(n_i, m_i)$.

$\Rightarrow gcd(a^2, b^2) = f_1^{j_1} \cdot f_2^{j_2} \cdot \ldots f_r^{j_r}$ where $j_i = 2k_i$, as squaring a and b is as simple as doubling the exponents to which each of the factors are raised.

Similarly, we can say that $gcd(a, b)^2 = f_1^{2k_1} \cdot f_2^{2k_2} \cdot \ldots f_r^{2k_r}$.

$\Rightarrow gcd(a^2, b^2) = gcd(a, b)^2$.

44. If $2^n - 1$ is a prime, prove that n itself is a prime.

Let's prove this by contradiction.

Let $n = ab$ and $1 < a \leq b$.

For the polynomial $2^{ab} - 1$ where $a, b \in \mathbb{N}$, $2^{ab} - 1 = (2^a - 1) \cdot (1 + 2^a + 2^{2a} + 2^{3a} + \ldots 2^{a(b-1)})$ due to the existence of a factorization.

Because n is composite, $(2^a - 1) \neq 1$ and $(2^a - 1) | (2^n - 1)$ which contradicts $2^n - 1$'s primality.

2.1

In [1]:
```
# Recursive form of gcd
def gcd(a, b):
    return b if a == 0 else gcd(b%a, a)

# List comprehension to find number of coprimes less than n
def tot(n):
    return len([i for i in range(n) if gcd(n, i) == 1])
```

10. Evaluate $\phi(m)$ for $m \in \{1, 2, 3...12\}$.

In [2]:
```
for i in range(1,13):
    print("ϕ({:2}) = {}".format(i, tot(i)))
```

```
ϕ( 1) = 1
ϕ( 2) = 1
ϕ( 3) = 2
ϕ( 4) = 2
ϕ( 5) = 4
ϕ( 6) = 2
ϕ( 7) = 6
ϕ( 8) = 4
ϕ( 9) = 6
ϕ(10) = 4
ϕ(11) = 10
ϕ(12) = 4
```

11. Find the least positive integer x such that $13|(x^2 + 1)$.

In [3]:
```
print([i for i in range(100) if (i ** 2 + 1) % 13 == 0][0])
```

```
5
```

12. Prove that 19 is not a divisor of $4n^2 + 4$ for any integer n.

Let us assume that this is not the case; i.e. $\exists n \in \mathbb{Z} : 19|4n^2 + 4$.

$$19|4n^2 + 4 \implies 4n^2 + 4 \equiv 0 \mod 19$$
$$\implies 4n^2 \equiv -4 \mod 19$$
$$\implies n^2 \equiv -1 \mod 19 \text{ because 4 has an inverse mod 19.}$$

Now, let us consider the group $\frac{\mathbb{Z}}{19\mathbb{Z}}^*$. Notice that this group has order $18 \implies \forall \text{ elements } e \in \frac{\mathbb{Z}}{19\mathbb{Z}}^*$, the order of e divides 18.

However, $[n]^2 = [-1] \implies [n]$ has order 4 and $4 \nmid 18$.

Therefore, $[n]$ cannot possibly be in the group.

14. Show that $7|(3^{2n+1} + 2^{n+2})$ for all n.

Let's work in group $\frac{\mathbb{Z}}{7\mathbb{Z}}$.

We seek to prove that $[3]^{2n+1} + [2]^{n+2} = [0]$.

$[3]^{2n+1} + [2]^{n+2} = [3]^{2n}[3]^1 + [2]^n[2]^2 = [2]^n[3] + [2]^n[4] = [2]^n([3] + [4]) = [2]^n([0]) = [0]$.

18. Show that if $p \equiv 3(\mod 4)$, then $\frac{p-1}{2}! \equiv \pm 1(\mod p)$

$(p-1)! = 1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \ldots (p-1) \equiv -1 \mod p$ by Wilson's Theorem.

This can be equivalently written as $(\frac{p-1}{2}!)((-1)^{\frac{p-1}{2}}\frac{p-1}{2}!)$ which, when p is of form $4n+3$, must be $-((\frac{p-1}{2})!)^2$ because $\frac{4n+2}{2} \equiv 1 \mod 2$.

$\implies (p-1)! = -((\frac{p-1}{2})!)^2 \equiv -1 \mod p \implies ((\frac{p-1}{2})!) = \pm 1 \mod p$.