Prime Factors, Divisors, and Friends

Wednesday, July 15

Prime Factors and Divisors

1. Find the number of divisors of the following numbers:

   (a) 80
   (b) 430
   (c) 256
   (d) 143
   (e) 10!
   (f) 6^18

2. How many times is 100! divisible by 7?
3. Define $\binom{p}{n}$ by $\frac{p!}{n!}(p-n)!$. Show that if p is prime and $1 < n < p$ then $\binom{p}{n}$ is divisible by p.
4. For what numbers n does $d(n) = 2$ hold?
5. For what numbers n does $d(n) = 3$ hold?
6. For what numbers n does $d(n) = 4$ hold?
7. Show that if $\gcd(a, b) = 1$ then $d(ab) = d(a)d(b)$.
8. Show that $d(n) \leq 2\sqrt{n}$ for all n.
9. There are a hundred lights in a row, numbered 1 to 100. All of them are currently off. You flip the switches for all lights with numbers divisible by 1. Then you do the same for all lights with numbers divisible by 2, 3, ..., 99, 100. How many lights are now on?

Euler's Phi Function

1. Show that $\varphi(p) = p - 1$.
2. Show that $\varphi(p^n) = p^n - p^{n-1} = p^n(1 - 1/p)$.
3. Show that if $\gcd(a, b) = 1$ then $\varphi(ab) = \varphi(a)\varphi(b)$.
4. Show that $\varphi(n) = n \cdot \prod_{p|n}(1 - \frac{1}{p})$.
5. Show that if $\gcd(a, b) = 1$ then $a^{\varphi(b)} \equiv 1 \pmod{b}$.
6. Find $\varphi(15)$ and evaluate $2^{66} \pmod{15}$.
7. Make multiplication tables for $\mathbb{Z}_5^\times, \mathbb{Z}_8^\times, \mathbb{Z}_{10}^\times$, and $\mathbb{Z}_{12}^\times$. Make observations.
8. Make multiplication tables for $\mathbb{Z}_7^\times$ and $\mathbb{Z}_9^\times$. Make observations.

Proofs of the Infinitude of Primes

1. Show that $n! + 1$ must have a prime factor greater than n. Conclude that there are infinitely many primes.
2. Modify Euclid's proof to show that there are infinitely many primes of the form $4n + 3$.
3. Use Euclid's proof plus strong induction to show that if p_n is the n-th prime number then $p_n \leq 2^{2^n}$.

Mersenne Primes

1. If $2^p - 1$ is prime then $2^{p-1}(2^p - 1)$ is a perfect number.
2. (Euclid-Euler Theorem) All even perfect numbers are of the above form.
3. If $a \geq 3$ and $n \geq 2$ then $a^n - 1$ is composite.
4. If $2^p - 1$ is prime then p is prime.
5. (Harder) if p is an odd prime then the only factors of $2^p - 1$ are equivalent to 1 mod 2p.
6. Use the above result to find a new proof that there are infinitely many primes.

Fermat Primes

1. Besides F_0 and F_1, all Fermat numbers have last digit 7.
2. Show that Fermat numbers satisfy the following relations for $n \geq 1$:
   (a) $F_n = (F_{n-1} - 1)^2 + 1$
   (b) $F_n = F_{n-1} + 2^{2^{n-1}} \prod_{i=0}^{n-2} F_i$
   (c) $F_n = F_{n-1}^2 - 2(F_{n-2} - 1)^2$
   (d) $F_n = 2 + \prod_{i=0}^{n-1} F_i$
3. Use the last relation in the previous question to show that any two Fermat numbers are relatively prime. Conclude that there are infinitely many primes.
4. If $2^k + 1$ is an odd prime, then k is a power of 2.

Orders of Elements

1. Write $.123123123123123\ldots$ as a fraction.
2. Write 17/33 as a repeating decimal.
3. Find the orders of $1, 5, 13$, and 17 in $\mathbb{Z}_{36}^{\times}$.
4. Find the order of 10 in $\mathbb{Z}_{13}^{\times}$. What is the period length in the decimal expansion of 1/13?
5. If an element a has order n in $\mathbb{Z}_m^{\times}$, prove that $1, a, a^2, a^3, \ldots, a^{n-1}$ are all distinct mod m.
6. If $ord(a)$ and $ord(b)$ are relatively prime then $ord(ab) = ord(a) \cdot ord(b)$.
7. In general, $ord(ab) = lcm(ord(a), ord(b))$.