Prime Factors, Divisors, and Friends

Wednesday, July 15

Prime Factors and Divisors

1. Find the number of divisors of the following numbers:
   (a) 80
   $80 = 2^4 \cdot 5$, so 80 has $(4+1)(1+1) = 10$ divisors.
   (b) 430
   $430 = 2 \cdot 5 \cdot 43$ and so has $2 \cdot 2 \cdot 2 = 8$ divisors.
   (c) 256
   $256 = 2^8$ and so has 9 divisors.
   (d) 143
   $143 = 13 \cdot 11$, and so has 4 divisors.
   (e) 10!
   $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$, and so has $9 \cdot 5 \cdot 3 \cdot 2 = 270$ divisors.
   (f) 6^18
   $6^{18} = 2^{18} \cdot 3^{18}$ and so has $19^2 = 361$ divisors.

2. How many times is 100! divisible by 7?

   100! is divisible by 7 $\lfloor 100/7 \rfloor + \lfloor 100/49 \rfloor = 14 + 2 = 16$ times.

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.

   $p!$ is divisible by p but $n!$ and $(p-n)!$ (having only factors smaller than p) are not. By the uniqueness of prime factorization, $\binom{p}{n}$ is divisible by p.

4. For what numbers n does $d(n) = 2$ hold?

   Primes only.

5. For what numbers n does $d(n) = 3$ hold?

   Only when $n = p^2$ for p prime.

6. For what numbers n does $d(n) = 4$ hold?

   When $n = pq$ with p, q prime or when $n = p^3$ with p prime.

7. Show that if $\gcd(a, b) = 1$ then $d(ab) = d(a)d(b)$.

   One way to solve this: let Div(a), Div(b), and Div(ab) be the set of positive divisors of a, b, and ab, respectively. We will make a function $f : Div(a) \times Div(b) \to Div(ab)$ defined by $f(m, n) = mn$ and show that it is a bijection, thus showing that the two sets have the same numbers of elements.

   One-to-one: suppose that $mn = m'n'$. We want to show that $m = m'$ and $n = n'$. Since $m, m'|a$ and $n, n'|b$ but $\gcd(a, b) = 1$ we can say that $\gcd(m, n) = \gcd(m, n') = \gcd(m', n) = \gcd(m', n') = 1$. Since $mn|m'n'$ we know that $m|m'$, and similarly $m'|m$. Therefore $m = m'$ and so $n = n'$. This establishes that f is one-to-one.

   Onto: Let $k|ab$. We want to show that there exist $m|a$ and $n|b$ such that $mn = k$. Let $m = \gcd(a, k)$ and let $n = \gcd(b, k)$. $m|a$ and $n|b$ by definition of the gcd, and because $\gcd(a, b) = 1$ we know that $\gcd(a, k) \cdot \gcd(b, k) = \gcd(ab, k)$ (prove this!) Therefore $mn = \gcd(a, k) \cdot \gcd(b, k) = \gcd(ab, k) = k$, proving that f is onto.

   This shows that f is a bijection and therefore that $d(ab) = d(a)d(b)$.

8. Show that $d(n) \leq 2\sqrt{n}$ for all n.

   If $ab = n$ then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. There are at most $\sqrt{n}$ divisors of n less than or equal to $\sqrt{n}$, and they have at most $\sqrt{n}$ partners greater than or equal to $\sqrt{n}$... $2\sqrt{n}$ in total.

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?

   For you to solve!

Euler's Phi Function

1. Show that $\varphi(p) = p - 1$.

   If p is prime, then $\gcd(a, p) = 1$ for all $1 \leq a < p$, so for $p - 1$ elements in total.

2. Show that $\varphi(p^n) = p^n - p^{n-1} = p^n(1 - 1/p)$.

   A number a is relatively prime to p^n if and only if it is not divisble by p, so there are $p^n - p^n/p = p^n(1 - 1/p)$ such elements in total.

3. Show that if $\gcd(a, b) = 1$ then $\varphi(ab) = \varphi(a)\varphi(b)$.

   The number produced by solving a system of congruences $x \equiv m \pmod a, x \equiv n \pmod b$ has (by the Chinese Remainder Theorem) a unique solution mod ab, so solving such a system of congruences marked by (m, n) gives a bijection $\mathbb{Z}_a \times \mathbb{Z}_b \leftrightarrow \mathbb{Z}_{ab}$.

   Additionally, if $\gcd(n, a) = \gcd(m, b) = 1$ then the solution produced by the algorithm for the Chinese remainder theorem must be relatively prime to ab. Thus the function is also a bijection $\mathbb{Z}_a^\times \times \mathbb{Z}_b^\times \leftrightarrow \mathbb{Z}_{ab}^\times$.

4. Show that $\varphi(n) = n \cdot \prod_{p|n}(1 - \frac{1}{p})$.

   Give the prime factorization of n by $n = \prod_{i=1}^k p_i^{a_i}$. Then

$$\begin{aligned}
\varphi(n) &= \varphi(\prod_i p_i^{a_i}) \\
&= \prod_i \varphi(p_i^{a_i}) \\
&= \prod_i p_i^{a_i}(1 - 1/p) \\
&= \prod_i p_i^{a_i} \prod_i (1 - 1/p) \\
&= n \prod_i (1 - 1/p)
\end{aligned}$$

5. Show that if $\gcd(a, b) = 1$ then $a^{\varphi(b)} \equiv 1 \pmod b$.

   Let c be any number such that $\gcd(c, b) = 1$. Then since $\gcd(a, b) = 1$, we know that $\gcd(ac, b) = 1$ as well. So the function $f(c) = ac \pmod b$ gives a bijection from $\mathbb{Z}_b^\times$ to $\mathbb{Z}_b^\times$. Therefore

$$\begin{aligned}
\prod_{c \in \mathbb{Z}_b^\times} c &\equiv \prod_{c \in \mathbb{Z}_b^\times} ac \\
&\equiv a^{\varphi(b)} \prod_{c \in \mathbb{Z}_b^\times} c \pmod b
\end{aligned}$$

Dividing by the product on both sides (which we can do, since it is relatively prime to b), we get $1 \equiv a^{\varphi(b)}$.

6. Find $\varphi(15)$ and evaluate $2^{66} \pmod{15}$.

   $\varphi(15) = 15 \cdot (1/2) \cdot (4/5) = 8$, so $2^{66} = 2^{64} \cdot 2^2 \equiv 2^2 \equiv 4 \pmod{15}$.

7. Make multiplication tables for $\mathbb{Z}_5^\times, \mathbb{Z}_8^\times, \mathbb{Z}_{10}^\times$, and $\mathbb{Z}_{12}^\times$. Make observations.

   Done in class. The interesting thing to note is that the square of every element in $\mathbb{Z}_8^\times$ and $\mathbb{Z}_{12}^\times$ is 1, which is not the case in the other two groups.

8. Make multiplication tables for $\mathbb{Z}_7^\times$ and $\mathbb{Z}_9^\times$. Make observations.

$\mathbb{Z}_7^\times$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$\mathbb{Z}_9^\times$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

One thing to note is a symmetry in the tables…for example $5 \cdot 7 \equiv (-4)(-2) \equiv 4 \cdot 2$, so rotating the table 180 degrees keeps it the same.

See 4-2-sols for the proofs relating to the infinitude of primes. Remaining proofs to be given after tomorrow.

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 $p_n \le 2^{2^n}$.

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 $a \ge 3$ and $n \ge 2$ 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, $ord(ab) = lcm(ord(a), ord(b))$.