Chapter 5.1: Induction

Monday, July 13

Fermat's Little Theorem

Evaluate the following:

1. $2^{16} \pmod 5$

$$2^{16} \equiv (2^4)^4 \equiv 1^4 \equiv 1 \pmod 5$$

2. $3^{32} \pmod 7$

$$3^{32} \equiv (3^4)^8) \equiv 1^8 \equiv 1 \pmod 5$$

3. $2^{77} \pmod{19}$

$$2^{77} \equiv (2^{18})^4 \cdot 2^5 \equiv 1^4 \cdot 32 \equiv 13 \pmod{19}$$

4. $2^{18} \pmod{15}$

   $2^{18} \equiv 1 \pmod 3$ and $2^{18} \equiv 4 \pmod 5$, so solving the simultaneous equations (by whatever method you like) gives $2^{18} \equiv 4 \pmod{15}$.

5. $2^{25} \pmod{21}$

   $2^{25} \equiv 2 \pmod 3$ and $2^{25} \equiv 2 \pmod 7$, so solving the two equations gives $2 \equiv 2 \pmod{21}$.

6. $2^{100} \pmod{55}$

   $2^{100} \equiv 1 \pmod 5$ and $2^{100} \equiv 1 \pmod{11}$, so solving the two equations gives $2^{100} \equiv 1 \pmod{55}$.

(Hard) A composite number n is called a Carmichael number $b^{n-1} \equiv 1 \pmod n$ for every number b such that $\gcd(b, n) = 1$ (their existence is unfortunate, since it means that we cannot use FLT to tell for certain whether a number is prime). Prove: There is one and only one Carmichael number of the form $3 \cdot p \cdot q$, where p and q are prime numbers.
We know that if $n = 3pq$ is a Carmichael number and $\gcd(b, n) = 1$ then

$$\begin{aligned} b^{3pq-1} &\equiv 1 \pmod{3pq} \\ b^{3pq-1} &\equiv 1 \pmod 3 \\ b^{3pq-1} &\equiv 1 \pmod p \\ b^{3pq-1} &\equiv 1 \pmod q \end{aligned}$$

Using Fermat's Little Theorem on the last three equations in turn gives us

$$\begin{aligned} 2 &| 3pq - 1 \\ p - 1 &| 3pq - 1 \\ q - 1 &| 3pq - 1 \end{aligned}$$

The first just tells us that p and q must be odd. Then since $3pq-1 = 3pq-3q+3q-1 = 3q(p-1)+3q-1$ (and similarly $3pq-1 = 3p(q-1)+3p-1$), we can conclude

$$\begin{aligned} p-1 &| 3q-1 \\ q-1 &| 3p-1 \end{aligned}$$

Suppose (without loss of generality) that $p < q$. Then since $q-1|3p-1 < 3q-1$, we know that either $q-1 = 3p-1$ or $2(q-1) = 3p-1$. The first possibility would give $q = 3p$, contradicting the given that p was prime. Therefore $2(q-1) = 3p-1$.
We can then substitute this into the first statment: $p-1|3q-1 = 3q-3+2 = \frac{3}{2}(2(q-1))+2 = \frac{3}{2}(3p-1)+2$, so $(p-1)|\frac{9}{2}p+1/2$, or $2p-2|9p+1$, or $2p-2|9p+1-4(2p-2) = p+9$. Since $2p-2|p+9$ means that $2p-2 \leq p+9$, we must have $p \leq 11$. Since $p \neq 3$, checking the other cases 5, 7, and 11 show that $p = 11$ is the only option. Therefore $q = 17$, and the only Carmichael number of the form $3pq$ is $3 \cdot 11 \cdot 17 = 561$.

Induction

1. Prove that $1^2+2^2+3^2+\cdots+n^2 = \dfrac{n(n+1)(2n+1)}{6}$ for $n \geq 0$.

   Base case: it works for $n = 0$ since $0 = 0(0+1)(0+2)/6$.

   Inductive step. Suppose that the formula works for n. Then

$$\begin{aligned} (1^2+2^2+\cdots+n^2)+(n+1)^2 &= n(n+1)(2n+1)/6+n^2+2n+1 \\ &= \frac{2n^3+3n^2+2n+6n^2+12n+6}{6} \\ &= \frac{2n^3+9n^2+14n+6}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6} \end{aligned}$$

2. Prove that $1^3+2^3+3^3+\cdots+n^3 = \left(\dfrac{n(n+1)}{2}\right)^2$ for $n \geq 0$.

   Base case: it works for $n = 0$.

   Inductive step: suppose it works for n. Then

$$\begin{aligned} (1^3+2^3+\cdots+n^3)+(n+1)^3 &= \frac{n^2(n+1)^2}{4}+n^3+3n^2+3n+1 \\ &= \frac{n^4+2n^3+n^2+4n^3+12n^2+12n+4}{4} \\ &= \frac{n^4+6n^3+13n^2+12n+4}{4} \\ &= \frac{(n+1)^2(n+2)^2}{4} \end{aligned}$$

3. Prove that $1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n+1)!-1$ for $n \geq 1$.

   Base case: it works for $n = 1$.

   Inductive step: suppose it works for n. Then

$$\begin{aligned} (1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n!) + (n+1) \cdot (n+1)! &= (n+1)! - 1 + [(n+2) \cdot (n+1)! - (n+1)!] \\ &= (n+2)! - 1 \end{aligned}$$

4. Find a closed form for $\sum_{k=1}^{n}(-1)^k k^2$ and prove that it is correct.

   The first few terms are $-1, 3, -6, 10, -15, \ldots$, so guess that the formula is $(-1)^n n(n+1)/2$.

   Base case: The formula works for $n = 1$.

   Inductive step: suppose that it works for n. Then

$$
\begin{aligned}
\sum_{k=1}^{n+1}(-1)^k k^2 &= \sum_{k=1}^{n}(-1)^k k^2 + (-1)^{n+1}(n+1)^2 \\
&= (-1)^n n(n+1)/2 + (-1)^{n+1}(n^2+2n+1) \\
&= (-1)^{n+1}\frac{2n^2+4n+2-n^2-n}{2} \\
&= (-1)^{n+1}\frac{n^2+3n+2}{2} \\
&= (-1)^{n+1}\frac{(n+1)(n+2)}{2}
\end{aligned}
$$

5. For what integers is $2^n \geq n^3$ true? Prove it.

   True for $n = 0, n = 1$, but also for $n \geq 10$.

   Base case: $2^{10} = 1024 \geq 1000 = 10^3$.

   Inductive step: suppose that $2^n \geq n^3$. Then

$$
\begin{aligned}
2^{n+1} &= 2 \cdot 2^n \\
&= 2^n + 2^n \\
&\geq n^3 + n^3 \\
&\geq n^3 + 10n^2 \\
&\geq n^3 + 3n^2 + 3n + 1 \\
&= (n+1)^3
\end{aligned}
$$

   The step $n^3 + n^3 \geq n^3 + 10n^2$ relied on the fact that $n \geq 10$.

From 2 to many

1. Given that $ab = ba$, prove that $a^n b = ba^n$ for all $n \geq 1$. (Original problem had a typo.)

   Base case: $a^1 b = ba^1$ was given, so it works for $n = 1$.

   Inductive step: if $a^n b = ba^n$, then $a^{n+1} b = a(a^n b) = aba^n = baa^n = ba^{n+1}$.

2. Given that $ab = ba$, prove that $a^n b^m = b^m a^n$ for all $n, m \geq 1$ (let n be arbitrary, then use the previous result and induction on m).

   Base case: if $m = 1$ then $a^n b = ba^n$ was given by the result of the previous problem.

   Inductive step: if $a^n b^m = b^m a^n$ then $a^n b^{m+1} = a^n b^m b = b^m a^n b = b^m b a^n = b^{m+1} a^n$.

3. Given: if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$. Prove: if $a_i \equiv b_i \pmod{m}$ for $i = 1, 2, \ldots, n$, then $\sum_{i=1}^n a_i \equiv \sum_{i=1}^n b_i \pmod{m}$.

   Base case: When $n = 2$ the formula $a + c \equiv b + d \pmod{m}$ was already given.

   Inductive step: Supposing the formula works for n, we get

$$\begin{aligned}\sum_{i=1}^{n+1} a_i &= (\sum_{i=1}^{n} a_i) + a_{n+1} \\ &\equiv \sum_{i=1}^{n} b_i + b_{n+1} \\ &\equiv \sum_{i=1}^{n+1} b_i\end{aligned}$$

4. (Calculus) Suppose we know that $\frac{d}{dx} x = 1$ and that for any functions f and g, $(fg)' = f'g + fg'$. Prove that $\frac{d}{dx} x^n = nx^{n-1}$ for all $n \geq 1$.

   Base case: when $n = 1$, $\frac{d}{dx} x^1 = 1 = 1 \cdot x^0$.

   Inductive step: If $\frac{d}{dx} x^n = nx^{n-1}$, then

$$\begin{aligned}\frac{d}{dx} x^{n+1} &= (x \cdot x^n)' \\ &= x' \cdot x^n + (x^n)' \cdot x \\ &= x^n + nx^{n-1} \cdot x \\ &= (n+1)x^n\end{aligned}$$

5. Prove: $\overline{\bigcup_{i=1}^{n} A_i} = \bigcap_{i=1}^{n} \overline{A_i}$.

   Base case: When $n = 2$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$ is given by one of DeMorgan's Laws.

Inductive step: Suppose the formula works for n. Then

$$\begin{aligned}
\overline{\bigcup_{i=1}^{n+1} A_i} &= \overline{\bigcup_{i=1}^{n} A_i \cup A_{n+1}} \\
&= \overline{\bigcup_{i=1}^{n} A_i} \cap \overline{A_{n+1}} \\
&= \bigcap_{i=1}^{n} \overline{A_i} \cap \overline{A_{n+1}} \\
&= \bigcap_{i=1}^{n+1} \overline{A_i}
\end{aligned}$$

Recursion

1. Define a sequence a_n by $a_0 = 1$, $a_1 = 3$ and $a_n = a_{n-1} + 2 \cdot a_{n-2}$ for $n \geq 2$. Find a_6. Prove that $a_n = \dfrac{2^{n+2} + (-1)^n}{3}$.

a_0	a_1	a_2	a_3	a_4	a_5	a_6
1	3	5	11	21	43	85

Base case for proof by induction: The formula works for $n = 0$ and $n = 1$.

Inductive step: Suppose that the formula works for n AND $n + 1$. Then

$$\begin{aligned}
a_{n+2} &= a_{n+1} + 2a_n \\
&= \frac{2^{n+3} + (-1)^{n+1}}{3} + 2 \cdot \frac{2^{n+2} + (-1)^n}{3} \\
&= \frac{2 \cdot 2^{n+3} + (-1)^n}{3} \\
&= \frac{2^{n+4} + (-1)^{n+2}}{3}
\end{aligned}$$

Note that this time we needed to use the formula for both a_{n+1} and a_n, so we needed to prove two base cases.

2. Define a sequence a_n by $a_0 = 1$, $a_n = 2 \cdot a_{n-1} + 1$ if $n \geq 1$. Find a non-recursive formula for a_n and prove that it is correct.

The sequence goes $1, 3, 7, 15, 31, \ldots$ guess that it is equal to $2^{n+1} - 1$.

Prove the base case: it works for $n = 0$.

Inductive step: If it works for n, then $a_{n+1} = 2 \cdot a_n + 1 = 2 \cdot (2^{n+1} - 1) + 1 = 2^{n+2} - 2 + 1 = 2^{n+2} - 1$.

3. Prove: $\gcd(f_{n+1}, f_n) = 1$ for all $n \geq 0$.

   Proof: $\gcd(f_0, f_1) = \gcd(0, 1) = 1$ for the base case $n = 0$.

   Inductive step: use the fact that $\gcd(a, b) = \gcd(a - b, b)$. Then if the proposition holds for n, we have $\gcd(f_{n+2}, f_{n+1}) = \gcd(f_{n+2} - f_{n+1}, f_{n+1}) = \gcd(f_n, f_{n+1}) = 1$.

4. Prove that $f_1^2 + f_2^2 + \cdots + f_n^2 = f_n f_{n+1}$ for $n \geq 1$.

   Base case: it works for $n = 1$ since $f_1^2 = 1 \cdot 1 = f_1 f_2$.

   Inductive step: if the formula holds for n, then

$$\begin{aligned}(f_1^2 + f_2^2 + \cdots + f_n^2) + f_{n+1}^2 &= f_n f_{n+1} + f_{n+1} f_{n+1} \\ &= f_{n+1}(f_n + f_{n+1}) \\ &= f_{n+1} f_{n+2}\end{aligned}$$

5. Prove that $f_1 + f_3 + \cdots + f_{2n-1} = f_{2n}$ for $n \geq 1$. (Original problem had a typo.)

   Base case: $f_1 = 1 = f_2$ when $n = 1$.

   Inductive step: if the formula holds for n, then

$$\begin{aligned}(f_1 + f_3 + \cdots + f_{2n-1}) + f_{2n+1} &= f_{2n} + f_{2n+1} \\ &= f_{2n+2}\end{aligned}$$

6. Show that $f_{n+1} f_{n-1} - f_n^2 = (-1)^n$ for $n \geq 1$.

   Base case: when $n = 1$, we have $f_2 f_0 - f_1^2 = 0 - 1 = (-1)^1$.

   Inductive step: If the formula holds for n then

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

7. Prove that $f_n = (\alpha^n - \beta^n)/\sqrt{5}$, where $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$. (Hint: both α and β satisfy the equation $x^2 = x + 1$).

   Proof: It holds for f_0 and f_1, base cases $n = 0$ and $n = 1$.

   Inductive step: if it holds for n AND $n + 1$ then

$$\begin{aligned}f_{n+2} &= f_{n+1} + f_n \\ &= \frac{\alpha^{n+1} - \beta^{n+1}}{\sqrt{5}} + \frac{\alpha^n - \beta^n}{\sqrt{5}} \\ &= \frac{\alpha^n(\alpha + 1) - \beta^n(\beta + 1)}{\sqrt{5}} \\ &= \frac{\alpha^{n+2} - \beta^{n+2}}{\sqrt{5}}\end{aligned}$$

8. Prove that $f_{m+n} = f_{m-1}f_n + f_m f_{n+1}$. (fix n arbitrarily, then use induction on m)

   Base case: when $m = 1$ the formula becomes $f_{n+1} = f_0 f_n + f_1 f_{n+1}$, which is true because $f_0 = 0$ and $f_1 = 1$.

   Inductive step: Suppose the formula holds for m. Then

$$\begin{aligned} f_{(m+1)+n} &= f_{m+(n+1)} \\ &= f_{m-1}f_{n+1} + f_m f_{n+2} \\ &= f_{m-1}f_{n+1} + (f_m f_{n+1} + f_m f_n) \\ &= (f_{m-1} + f_m)f_{n+1} + f_m f_n \\ &= f_m f_n + f_{m+1}f_{n+1} \\ &= f_{(m+1)-1}f_n + f_{m+1}f_{n+1} \end{aligned}$$

9. Prove (now using induction on n) that $f_m | f_{mn}$ for all $n \geq 1$.

   Base case: When $n = 1$ this is just $f_m | f_m$, which is clearly true.

   Inductive step: suppose $f_m | f_{mn}$. Then

$$\begin{aligned} f_{m(n+1)} &= f_{mn+m} \\ &= f_{mn-1}f_m + f_{mn}f_{m+1}. \end{aligned}$$

   Since f_m and (by the inductive hypothesis) f_{mn} are both divisible by f_m, the linear combination (and therefore $f_{m(n+1)}$) is also divible by f_m.

10. Prove that $\gcd(f_m, f_n) = f_{\gcd(m,n)}$.

    Let $n = qm + r$. Since $f_m | f_{qm}$ (from the previous problem), we know that

$$\begin{aligned} \gcd(f_m, f_n) &= \gcd(f_m, f_{qm+r}) \\ &= \gcd(f_m, f_{qm-1}f_r + f_{qm}f_{r+1}) \\ &= \gcd(f_m, f_{qm-1}f_r), \end{aligned}$$

    Then since $f_m | f_{qm}$ but $\gcd(f_{qm}, f_{qm-1}) = 1$, we can conclude that $\gcd(f_m, f_n) = \gcd(f_m, f_{qm-1}f_r) = \gcd(f_m, f_r)$. This allows us to use a process similar to the Euclidean Algorithm and continue until we hit the greatest common divisor.

    In particular, this means that if p is a prime number, then f_p shares a common divisor with f_n if and only if $p | n$ (and if $p | n$ then $f_p | f_n$). In particlar, we know that $f_3 = 2$, so (since 3 is prime), the even Fibonacci numbers will be precisely those of the form f_{3k} for $k \in \mathbb{Z}$.