Jan 16th

Theorem (Fundamental Theorem of Arithmetic)
Every natural number >1 can be written as a product of

$$n=\underbrace{p_1\cdots p_k}_{\text{prime}}$$

$12=2\cdot 3\cdot 3$

Proof: Sps there exist numbers with non unique factorizations into primes
Let N be the smallest such number
$\underbrace{2,3,4,5\cdots N-1}_{\text{have unique factorizations}}, N$ has at least two factorizations

$N=\underbrace{p_1\cdots p_k}_{\text{primes}}=\underbrace{q_1\cdots q_h}_{\text{primes}}$ different factorizations

Claim: $p_i\neq q_j$ for any i,j
Why can't we have $p_1=q_1$?
if $p_1=q_1 \Rightarrow \frac{N}{p_1}=p_2\cdots p_k=\frac{N}{q_1}=q_2\cdots q_h<N$

$\frac{N}{p_1}$ natural number $<N$
with two distinct factorizations. Contradiction since N is the smallest such number.
So $p_i\neq q_j$, for any i,j in particular $p_1\neq q_1$
$\Rightarrow$ two possibilities $p_1>q_1$ or $p_1<q_1$,
Cases1: $p_1>q_1$ Case 2 $p_1<q_1$.

Look at $N-q_1p_2\cdots p_k=M$
$M>N>0$ natural number $N=p_1p_2\cdots p_k$
$M=p_1p_2\cdots p_k-q_1p_2\cdots p_k=(p_1-q_1)p_2\cdots p_k$
$M=(p_1-q_1)p_2\cdots p_k<N$

$(p_1-q_1)<N \Rightarrow$ has a unique prime factorization
$p_1-q_1=\underbrace{a_1\cdots a_n}_{\text{primes}}$
$M=\underbrace{(a_1\cdots a_n)}_{p_1-q_1}p_2\cdots p_k$

$M=N-q_1p_2\cdots p_k=\underbrace{q_1q_2\cdots q_h}_{N}-q_1p_2\cdots p_k=q_1\underbrace{(q_2\cdots q_k-p_2\cdots p_k)}_{b_1\cdots b_s \text{ prime factorizations}}=q_1b_1\cdots b_s$

$M=\underbrace{a_1\cdots a_n p_2\cdots p_k}_{\text{two factorizations of } M \text{ and } M<N}=q_1b_1\cdots b_s$

$\Rightarrow$ these two factorizations are the same up to reordering q_1 should appear in the 1st factorization somewhere $q_1\neq p_j$ for any $j \Rightarrow q_1=a_i$ for some i.

$p_1 \cdot q_1 = a_1 \cdots a_i \cdots a_n = q_i C$ - natural numbers
($a_i = q_i$)

... Check 4.1 for detailed proof.

Corollary: If p is prime and $p|ab$ then $p|a$ or $p|b$

Note: $a|b$ means a divides b

Ex: $3|6\cdot 2 \Rightarrow 3|6$ or $3|2$
✓ ✗

Is this true if p is not prime?
$12|3\cdot 8 = 24$ $12|3$, $12|8$
✗ ✗

$12|3\cdot 4$ but $12\nmid 3$, $12\nmid 4$

Proof: Let $p|a\cdot b$ (p prime) $\Rightarrow a\cdot b = pc = p\, q_1\cdots q_s$ (primes)

$a = m_1 \cdots m_m$ (primes)

$ab = m_1 \cdots m_m t_1 \cdots t_n$

$b = t_1 \cdots t_n$ (primes)

$\Rightarrow p$ is one of m_i's or p is one of t_j's
$\Rightarrow p|a$ or $p|b$

Corollary: if $n>1$ is a natural number as $n = p_1^{k_1} \cdots p_i^{k_i}$ (distinct primes) and this factorization is unique.

$60 = 4\cdot 15 = 4\cdot 3\cdot 5 = 2\cdot 2\cdot 3\cdot 5 = 2^2\cdot 3^1\cdot 5^1$

> If $p_1 \neq p_2$ are primes and $p_1|a$ and $p_2|a \Rightarrow p_1 p_2|a$
> ex: $2|24$, $3|24 \Rightarrow 2\cdot 3 = 6|24$

Is this true if p_1, p_2 not prime?
Example: $4|12$, $6|12$, but $4\times 6 = 24 \nmid 12$

Modular Arithmetic

Def'n: a, b, m integers
We say $a \equiv b \pmod m$
a is equivalent to b modulo m if $m \mid a-b$

Ex: $12 \equiv 2 \pmod 5$
$5 \mid 12-2=10$
$12 \not\equiv 4 \pmod 5$ $\quad 5 \nmid 12-4=8$
$9 \equiv -1 \pmod 5$ $\quad 9-(-1)=10$, divided by 5 is

$-3\ (-2)\ -1\ 0\ 1\ 2\ (3)\ 4\ 5\ 6\ 7\ (8)\ 9\ 10\ 11\ 12\ (13)$

Which numbers are equivalent to 3 mod 5
$3+5k$, $k=0, \pm1, \pm2, \pm3 \cdots$

Properties: $a \equiv b \pmod m$, $c \equiv d \pmod m$ then
$a+c \equiv b+d \pmod m$
$a-c \equiv b-d \pmod m$
$ac \equiv bd \pmod m$

Ex: $12 \equiv 2 \pmod 5$
$3 \equiv -2 \pmod 5$

$12+3 \equiv 0 \pmod 5$
$12-3 = 4 \pmod 5$
$12 \cdot 3 \equiv 2 \cdot (-2) \pmod 5$

Proof: $a \equiv b \pmod m$ means $a-b=mk$, $a=b+mk$
$c \equiv d \pmod m$ means $c-d=m \cdot l$, $c=d+ml$

$a+c=b+d+m(k+l)$
$(a+c)-(b+d)=m(k+l)$
$a+c \equiv b+d \pmod m$

$ac=(b+mk)(d+ml)=bd+mkd+bml+m^2kl$

$ac-bd=m(kd+bl+mkl)$
$\Rightarrow ac \equiv bd \pmod m$

Does this work mod m?

$ac \equiv bc \pmod m \Rightarrow a \equiv b \bmod m$ NO

$c \not\equiv 0 \bmod m$

ex: $m=4$ $c=2 \not\equiv 0 \bmod 4$

$a=2$ $b=0$

$ac=4 \equiv bc=0 \bmod 4$

but $a \not\equiv b \bmod 4$

$2 \not\equiv 0 \bmod 4$

Corollary: If $a \equiv b \bmod m \Rightarrow a^n \equiv b^n \bmod m$ for any n

Proof. We use mathematical induction. The case n = 1 is the hypothesis. Assume that the result is true for n = k; that is, ak ≡ bk (mod m). Since a ≡ b(mod m), using part (ii) of Theorem 3.1.5 gives a · ak = b · bk (mod m), or ak+1 ≡ bk+1 (mod m).

APPLICATION

$2^{100} \bmod 7 = ?$

$2^1 \equiv 2 \bmod 7$

$2^2 \equiv 4 \bmod 7$

$2^3 \equiv 1 \bmod 7$

$(2^3)^k \equiv 1^k \bmod 7$

$2^{3k} \equiv 1^k = 1 \bmod 7$

$2^{100} = 2^{1+99} = 2^1 \cdot 2^{99} = 2^1 \cdot (2^3)^{33} \equiv 2 \cdot 1 = 2 \bmod 7$

2^{100} What is the last digit?

$2^{100} \bmod 10$

$2^1 \equiv 2 \bmod 10$

$2^2 \equiv 4 \bmod 10$

$2^3 \equiv 8 \bmod 10$

$2^4 \equiv 6 \bmod 10$

$2^5 \equiv 2 \bmod 10$

$2^6 \equiv 4 \bmod 10$

$2^9 \equiv 8 \bmod 10$

etc.

$2^{4k+1} \equiv 2 \bmod 10$

$2^{4k+2} \equiv 4 \bmod 10$

$2^{4k+3} \equiv 8 \bmod 10$

$2^{4k+4} \equiv 6 \bmod 10$

$2^{100} = (2^4)^{25} \equiv 6 \bmod 10$

$2^{102} = 2^2 \cdot 2^{100} \equiv 4 \cdot 6 \equiv 4 \bmod 10$

$2^{3^{101}} \pmod 5 \equiv ?$

↳ means $2^{(3^{101})}$

$2^1 \equiv 2 \bmod 5$
$2^2 \equiv 4 \bmod 5$
$2^3 \equiv 3 \bmod 5$
$2^4 \equiv 1 \bmod 5$

$2^{4k+1} \equiv 2 \bmod 5$
$2^{4k+2} \equiv 4 \bmod 5$
$2^{4k+3} \equiv 3 \bmod 5$
$2^{4k} \equiv 1 \bmod 5$

we need to figure out what is $3^{101} \bmod 4$

$3^1 \equiv -1 \bmod 4$
$3^2 \equiv 1 \bmod 4$
$3^3 \equiv -1 \bmod 4$
$3^4 \equiv 1 \bmod 4$

$3^k \equiv (-1)^k$ $\begin{cases} +1 & \text{if } k \text{ is even} \\ -1 & \text{if } k \text{ is odd} \end{cases}$

$3^{101} \equiv -1 \bmod 4$ b/c 101 is odd

$\Rightarrow 3^{101} \equiv 3 \bmod 4$

$3^{101} = 4k+3$ for some k

$\Rightarrow 2^{3^{101}} = 2^{4k+3} \equiv 3 \bmod 5$

Theorem: n natural number n is divisible by 9 iff the sum of its digits is divisible by 9.

$27 = 2+7 = 9$

35 - not divisible $3+5=8$ ×

3456 $3+4+5+6 = 18 = 9 \cdot 2$
divisible by 9.

$n = \overline{a_k a_{k-1} \cdots a_0} = a_0 \cdot 1 + a_1 \cdot 10 + \cdots + a_k \cdot 10^k$
$0 \le a_i \le 9$

$237 = 7 + 3 \cdot 10 + 2 \cdot 10^2$
$3456 = 6 + 5 \cdot 10 + 4 \cdot 10^2 + 3 \cdot 10^3$

proof see next page.

then: $a_0 10^0 + a_1 10^1 + \cdots + a_k 10^k \equiv a_0 + \cdots + a_k \pmod 9$

$10 \equiv 1 \mod 9$

$100 \equiv 1 \mod 9$

... ...

$\Rightarrow 10^k \equiv 1 \mod 9$

$10^k \cdot a^k \equiv a^k \pmod 9$ for any k and any a_k

$+ a_0 10^0 \equiv a_0 \mod 9$

$+ a_1 10^1 \equiv a_1 \mod 9$

$+ a_2 10^2 \equiv a_2 \mod 9$

... ...

$a_0 10^0 + a_1 10^1 + \cdots + a_k 10^k \equiv a_0 + a_1 + \cdots + a_k \mod 9$