Math 312, Lecture 15, 7/6/2011

Tips: $3^x \cdot 3^y = 3^{x+y} \neq 3^{x \cdot y}$, $(3^x)^2 \neq 3^{x^2}$ | $a^x \cdot b^x = (ab)^x$

① $(3^x)^y = 3^{xy} \neq 3^{x^y} = 3^{(x^y)}$. | $a^x \cdot b^y \neq (ab)^{xy}$

② $a \cdot b \mid x^3$ does not make a, b cubes $(8 = 4 \cdot 2)$

~~unless~~ (it does if $(a,b) = 1$)

In the exam, solution to 5(b) has several steps:

(1) factor $x^3 = (y+1)(y-1)$

(2) show $(y+1, y-1) = 1$

(3) use unique factorization to ~~count~~ evaluate exponents of primes in $y \pm 1$, see that they are cubes

Last time: If $(m,n)=1$

$$\left\{\begin{matrix}\text{divisors}\\ \text{of } mn\end{matrix}\ d\right\} \overset{1:1}{\longleftrightarrow} \left\{\begin{matrix}\text{divisors}\\ d_1 \text{ of } m\end{matrix}\right\} \times \left\{\begin{matrix}\text{divisors}\\ d_2 \text{ of } n\end{matrix}\right\}$$

$$d \qquad = d_1 \cdot d_2$$

$\Rightarrow \tau(mn) = \tau(m)\,\tau(n)$

$\Rightarrow$ If f, g mult. so is $f*g = g*f$.

Thm: $I * \mu = \delta$ (hence $f * I = g \Leftrightarrow f = \mu * g$)

Pf: (1) Saw μ is multiplicative

$$\mu(n) = \begin{cases} 1 & n \text{ pdt of even \# of distinct primes} \\ -1 & n \text{ pdt of odd \# of distinct primes} \\ 0 & \text{else, i.e. if } p^2 \mid n \end{cases}$$

(2) use multiplicativity: I is completely mult.

so $I*\mu$ is mult.

δ is completely mult: if $m=n=1$ then $\delta(mn)=1 = \delta(m)\,\delta(n)$

if $m>1$ or $n>1$ then $mn>1$ and $\delta(mn)=0=\delta(m)\,\delta(n)$

So, for any $n = \prod_p p^{e_p}$

$$(I*\mu)(n) = \prod_p (I*\mu)(p^{e_p})$$

$$\delta(n) = \prod_p \delta(p^{e_p})$$

So if $(I*\mu)(p^e) = \delta(p^e)$ for all p, all e

then $(I*\mu)(n) = \delta(n)$ for all n

(3) **Prime powers:** let $e \geq 1$. Then $p^e > 1$, so $\delta(p^e) = 0$

$$(\mu * I)(p^e) = \mu(1) \cdot I(p^e) + \mu(p) I(p^{e-1}) + \mu(p^2) I(p^{e-2}) + \cdots + \mu(p^e) I(1)$$

$$= 1 \cdot 1 + (-1) \cdot 1 + 0 \cdot 1 + 0 \cdot 1 + \cdots$$

$\mu(1) = 1$ $\mu(p) = -1$ $\mu(p^k) = 0$ if $k \geq 2$

$$= 1 - 1 + 0 + 0 + \cdots = 0 = \delta(p^e)$$

$\blacksquare$

Remark: How many factorizations does p^e have?

$\tau(p^e) = e+1$ (divisors are $p^0, p^1, p^2, \ldots, p^e$)

$$\Rightarrow \tau\left(\prod_p p^{e_p}\right) \underset{\substack{\uparrow \\ \tau \text{ is mult.}}}{=} \prod_p \tau(p^{e_p}) = \prod_p (e_p + 1)$$

Problem: $\tau(n) = 77$, $6 \mid n$. What is n?

notice: τ is multiplicative, so think in terms of prime factorization

in these co-ords $n = 2^a \cdot 3^b \cdot m$ $(m, 6) = 1$

(or $n = 2^a \cdot 3^b \cdot \prod_{p \geq 5} p^{e_p}$)

notice: $77 = 7 \cdot 11$ at most two non-1 factors in $\tau(n) = \prod_p (e_p + 1)$

Solution: Write $n = 2^a 3^b \cdot m$ with $(m, 2 \cdot 3) = 1$ by unique factorization

Then $\tau(n) = \tau(2^a) \cdot \tau(3^b) \cdot \tau(m) \underset{\substack{\uparrow \\ \tau \text{ is mult}}}{=} (a+1)(b+1) \cdot \tau(m)$

$2, 3 \mid n$ so $a \geq 1$, $b \geq 1$, so $a+1 \geq 2$, $b+1 \geq 2$

so $7 \cdot 11 = 77 = (a+1) \cdot (b+1) \cdot \tau(m)$

with $a+1, b+1 \geq 2$

the only way to factor 77 into factors both not 1 is $77 = 7 \cdot 11$ or $11 \cdot 7$ so:

either $a+1 = 7$, $b+1 = 11$ in any case $\tau(m) = 1$

or $a+1 = 11$, $b+1 = 7$

$\Rightarrow$ either $\begin{cases} a = 6 \\ b = 10 \end{cases}$ or $\begin{cases} a = 10 \\ b = 6 \end{cases}$ in any case $m = 1$ (if $m > 1$ $1 \neq m$ both divide m so $\tau(m) \geq 2$)

$\Rightarrow$ either $n = 2^6 \cdot 3^{10}$ or $n = 2^{10} \cdot 3^6$

Perfect numbers

Recall (WW) n is <u>abundant</u> if $\sigma(n) > 2n$

<u>deficient</u> if $\sigma(n) < 2n$

<u>perfect</u> if $\sigma(n) = 2n$

(notions from numerology in ancient Greece)

$$\sigma(n) = \sum_{d|n} d = (N * I)(n) \quad \text{is mult.}$$

So $\sigma\left(\prod_p p^{e_p}\right) = \prod_p \sigma(p^{e_p})$.

Also $\sigma(p^e) = 1 + p + p^2 + \cdots + p^e = \dfrac{p^{e+1} - 1}{p-1}$

Ex. $\sigma(6) = \sigma(2)\cdot\sigma(3) = \dfrac{2^2-1}{2-1} \cdot \dfrac{3^2-1}{3-1} = 3 \cdot 4 = 12 = 2 \cdot 6$

$\sigma(28) = \sigma(4)\cdot\sigma(7) = \dfrac{2^3-1}{2-1} \cdot \dfrac{7^2-1}{7-1} = 7 \cdot 8 = 2 \cdot 28$

<u>Open:</u> Do there exist odd perfect numbers?

We'll study even ones: $n = 2^s \cdot m$, m odd, $s \geq 1$

$(2^s, m) = 1$: ~~every divisor of 2^s other that~~
only prime dividing 2^s does not divide m

So $\sigma(2^s \cdot m) = \sigma(2^s)\cdot\sigma(m) = \dfrac{2^{s+1}-1}{2-1} \cdot \sigma(m) = (2^{s+1}-1)\cdot\sigma(m)$

If n is perfect, $\sigma(n) = 2n$ so: $(2^{s+1}-1)\cdot\sigma(m) = 2^{s+1} \cdot m$

so $2^{s+1} \mid (2^{s+1}-1)\cdot\sigma(m)$ But $(2^{s+1}, 2^{s+1}-1)=1$

so $2^{s+1} \mid \sigma(m)$ write $\sigma(m) = 2^{s+1}\cdot t$

get: $m = \frac{2^{s+1}-1}{2^{s+1}}\cdot\sigma(m) = (2^{s+1}-1)\cdot t$

$\sigma(m) = 2^{s+1}\cdot t$

If $t>1$ then $1, t, m$ distinct divisors of m

so $\sigma(m) \geq 1+t+m = 1+t+(2^{s+1}-1)\cdot t$

$= 1+\cancel{t}\cdot 2^{s+1}\cdot t - \cancel{t} = \sigma(m)+1$

It follows that $t=1$.

$\Rightarrow m = 2^{s+1}-1, \quad n = 2^s(2^{s+1}-1)$

$\sigma(m) = 2^{s+1} = 1+m$ so $1, m$ are only divisors of m

so m is prime

PS 2s If $m = 2^{s+1}-1$ is prime, then $s+1=p$ is prime
$s = p-1$

so $\boxed{n = 2^{p-1}(2^p-1) \text{ with } 2^p-1 \text{ a Mersenne prime}}$

Exs If n has this form $\sigma(n) = 2n$

so $2\cdot(2^2-1)$, $2^2\cdot(2^3-1)$, $2^4\cdot(2^5-1)$, $2^6\cdot(2^7-1)$, ... are perfect
$\quad 6 \qquad\quad 28$

Cryptography

Three parties: Alice, Bob, Eve

Alice has a message P ("plaintext") she would like to send to Bob.

Goal: ~~Bob~~ Do it in such a way that Bob learns P but Eve, who is eavesdropping, doesn't.

Formalize this: Alice has a function E ("Encryption") she will compute $C = E(P)$ ("ciphertext") send C to Bob

Both Eve and Bob know C, need to solve equation $C = E(x)$

Idea: this should be hard unless you have some secret knowledge: Bob has a fcn D ("~~enc~~ decryption")

s.t.: $D(C) = P$, i.e. $D(E(P)) = P$

Example: character ciphers

"HELLO" want to send it

treat each letter as a message, send separately

Encode alphabet as the residues $\{0, 1, 2, .., 25\}$ mod 26

$A \equiv 0, \; B \equiv 1, \; C \equiv 2, \; .., \; Z \equiv 25.$

HELLO $\to$ 7, 4, 11, 11, 14.

Caesar cipher: $E(P) \equiv P+3 \ (26)$

$E(H) = K, \; E(E) = H, \; E(L) = O, \; E(O) = R$

Alice sends KHOOR

Bob uses $D(P) = P-3$

secrets shift 3. Call it the "key".

Affine cipher: Any map $E(P) \equiv aP+b \pmod{26}$

(Key = numbers a, b). Decryptions solve $aP+b \equiv C$ for P

for this need a invertible (mod 26) then $P = D(C) \equiv \bar{a}(C-b)$

$\equiv \bar{a}C - \bar{a}b$

also affine

Remark: (ETAOIN) ~~note each~~ letters occur with distinct frequencies.

similarly TH, THE most common digraphs, trigraphs