Math 321

Q's (4.3 #11) $\log_2 3$ is irrational

$\boxed{\text{Pf}}$ (contradiction; idea $\log_2 3$ is rational $\equiv F$)

assume $\log_2 3$ is rational. (Means) $\log_2 3 = \frac{a}{b}$ $a,b \in \mathbb{Z}$, $b \neq 0$, no common fac.

$$2^x = y \leftrightarrow x = \log_2(y)$$

$$2^{a/b} = 3 \longleftrightarrow \frac{a}{b} = \log_2(3)$$

$$(3)^b = \left(2^{a/b}\right)^b \longrightarrow 3^b = 2^a = n$$

Contradiction #1 left is odd, right is even so
n is odd $\wedge$ even $\equiv F$

or #2 n has $\boxed{\text{two}}$ prime factorizations $3^b \wedge 2^a$
False by Fund. Th^m of arithmetic

---

things to do with prime factorizations..

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$
$$b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

ex
$$a = 2^2 \cdot 3^3 \cdot 11 = 2^2 3^3 5^0 7^0 11^1$$
$$b = 2 \cdot 5 \cdot 7 \cdot 11^3 = 2^1 3^0 5^1 7^1 11^3$$

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} \cdots p_n^{\min(a_n,b_n)}$$
$$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} \cdots p_n^{\max(a_n,b_n)}$$

$$\gcd(a,b) = 2^1 3^0 5^0 7^0 11^1$$
$$\operatorname{lcm}(a,b) = 2^2 3^3 5^1 7^1 11^3$$

$\boxed{\text{Th}^m}$ $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = a \cdot b$

Faster gcd(a,b)?

Euclidean Algorithm

$a = q \cdot b + r \qquad 0 \le r < b$

$\gcd(a,b) = \gcd(b,r)$

$\gcd(24, 14) = 2$	$24 = 1 \cdot 14 + 10$ ③
$\gcd(14, 10) = 2$	$14 = 1 \cdot 10 + 4$ ②
$\gcd(10, 4) = 2$	$10 = 2 \cdot 4 + \boxed{2}$ ①
$\gcd(4, 2) = 2$	$4 = 2 \cdot 2 + 0$

Bézout's Identity

$\gcd(a,b) = s \cdot a + t \cdot b \ , \quad s,t \in \mathbb{Z}$

1) $\gcd(24,14) = 2 \overset{①}{=} 10 - 2 \cdot 4 \overset{②}{=} 10 - 2(14 - 1 \cdot 10)$

$2 = 3 \cdot 10 - 2 \cdot 14 \overset{③}{=} 3(24 - 1 \cdot 14) - 2 \cdot 14$

$\gcd(24,14) = 2 = \underline{3} \cdot 24 - \underline{5} \cdot 14$

Multiplicative Inverse under mod m

College Algebra (and equality)

$a \cdot ? = 1$ (mult. Identity)

$a \cdot \left(\frac{1}{a}\right) = 1$

zero does not have an inv.

Number theory

$a \cdot ? \equiv_m 1$

ex $3 \cdot 4 \equiv_{11} 1$ so 4 is 3's inv. for mod 11

So $0 \equiv_{11} -18 \equiv_{11} -7 \equiv_{11} 4 \equiv_{11} 15 \equiv_{11} 26 \equiv_{11} \dots$

Q Does a have an inv. for mod m?

exist?

$$a \cdot a^{-1} \equiv_m 1$$

Yes if $\gcd(a, m) = 1$ (rel. prime)

Bézout's $\gcd(a,m) = \boxed{1 = s \cdot a + t \cdot m}$

take mod m

$$1 = s \cdot a + 0$$

So $s = a^{-1}$ under mod m

$1 = \gcd(6, 7)$ $\quad 7 = 1 \cdot 6 + \boxed{1}$

$\gcd(6, 1)$ $\quad 6 = 6 \cdot 1 + 0$

$$1 = 1 \cdot 7 - 1 \cdot 6$$

under mod 7 $\quad$ 6's inv. is $-1 \equiv_7 6$

Application: Cryptography

$\boxed{f \text{ is invertible}}$