Math 321

Q's / #11 4.3

$\log_2 3 = x$

$\boxed{2^x = 3}$ $\quad x$ is $\boxed{\text{not}}$ rational

pf assume x is rational $\quad x = \frac{a}{b}$ (blah, blah rules on a, b)

$2^{\frac{a}{b}} = 3 \to \boxed{2^a = 3^b} \equiv F$

$\to \underbrace{2 \cdot 2 \cdot \cdots \cdot 2}_{a \text{ of them}} = \underbrace{3 \cdot 3 \cdot \cdots \cdot 3}_{b \text{ of them}} = n$

n has two prime factorizations $\equiv F$. by $\boxed{\text{fund. th}^{a}}$

Q $\quad \gcd(a,b) = \gcd(b,r)$ $\quad$ Euclidean Algorithm

$a = q \cdot b + r$

$\gcd(44, 21) = \gcd(21, 2) = \gcd(2, 1) = 1$

$44 = 2 \cdot 21 + 2$

$21 = 10 \cdot 2 + \boxed{1}$

$2 = 2 \cdot 1 + 0$

$\gcd(44,21) = 1 = 21 - 10 \cdot \underset{44 - 2 \cdot 21}{2} = 21 - 10(44 - 2 \cdot 21)$

$\gcd(44,21) = \boxed{1 = (-10)44 + (21)21}$

$\boxed{\text{Bézout's Identity}}$ $\quad \gcd(a,b) = s \cdot a + t \cdot b$

$s, t \in \mathbb{Z}$

why? if $\gcd(a,b)=1$

$$1 = s\cdot a + t\cdot b$$

take mod b $\quad 1 \bmod b = (s\cdot a + \underline{t\cdot b}^{\,0}) \bmod b$

$$1 = s\cdot a \bmod b$$

$$s\cdot a \underset{b}{\equiv} 1$$

So $\boxed{\text{s is a's multiplicative inverse mod b}}$

ex $\quad 1 \underset{21}{\equiv} \underline{(-10)\cdot 44}$

$\boxed{\text{-10 is 44's mult. inverse mod 21}}$

21 is 21's mult. inverse mod 44

ex Solve: $44x + 17 \underset{21}{\equiv} 19$

$$-17 \qquad -17$$

$$44x \underset{21}{\equiv} 2$$

$$\underline{(-10)}44x \underset{21}{\equiv} (-10)(2)$$

$$x \underset{21}{\equiv} -20 \underset{21}{\equiv} \boxed{1}$$

☆

(ex) $\gcd(92,26) = \gcd(26,14) = \gcd(14,12) = \gcd(12,2) = 2$

$92 = 3\cdot 26 + 14$ $\qquad$ $2 = 14 - 1\cdot 12$

$26 = 1\cdot 14 + 12$ $\qquad$ $2 = 14 - 1(26 - 1\cdot 14)$

$14 = 1\cdot 12 + \boxed{2}$ $\qquad$ $2 = 2\cdot 14 - 1\cdot 26$

$12 = 6\cdot 2 + 0$ $\qquad$ $2 = 2(92 - 3\cdot 26) - 1\cdot 26$

$\qquad$ $2 = 2\cdot 92 - 7\cdot 26$

Def $\gcd(a,b) = 1$

a,b are called relatively prime

(no common factors)

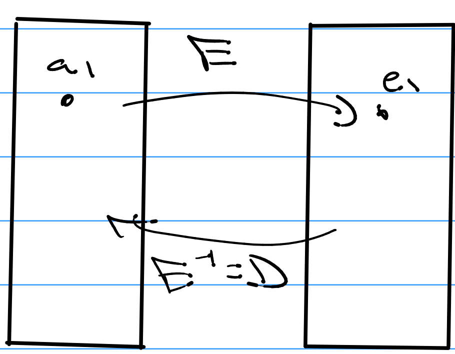
$\mathbb{Q} = \{ \frac{a}{b} \mid a,b \in \mathbb{Z},\ b \neq 0,\ \gcd(a,b) = 1 \}$

4.6 Cryptography

DUHK Attack

Don't Use Hard-coded Keys!

Study of invertible functions



plain text $\qquad$ cyphered text (encrypted text)

① given E and E^{-1} is "easy" to find (private key crypto)

② given E and E^{-1} is "hard" to find (public key crypto)