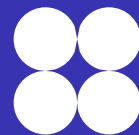


Lab 6

CS 135



Problem 1 from pset 6

d. $(a|bc \wedge \gcd(a, b) = 1) \Rightarrow a|c$

e. $\gcd(a, b) = \gcd(b, \text{rem}(a, b))$, where $\text{rem}(a, b)$ is the remainder when a is divided by b .

Problem 1 Answer Key

- d. $(a|bc \wedge \gcd(a, b) = 1) \Rightarrow a|c$
- e. $\gcd(a, b) = \gcd(b, \text{rem}(a, b))$, where $\text{rem}(a, b)$ is the remainder when a is divided by b .

D. From the LHS we have that $bc = ax$, and $\exists s, t: sa + tb = 1$.
Multiplying both sides by c , we have: $sac + tbc = c$.
Substituting for bc , this becomes $sac + tax = c$, or $a(sc + tx) = c$. From this last equation it follows that $a \mid c$.

E. From $a = bq + r$, $0 \leq r < b$ we see that every divisor of a and b must also divide r . Furthermore, every divisor of b and r must also divide a . Therefore $\gcd(a, b) = \gcd(b, r)$.

Problem 2 Pulverizer

Use the Pulverizer to express $\gcd(221, 91)$ as a linear combination of 221 and 91.

Problem 2 Answer Key

$$\gcd(221, 91)$$

$$13 = 91 - 2 \cdot 39$$

$$\gcd(91, 39)$$

$$221 = 91 \cdot 2 + 39$$

$$= 91 - 2(221 - 2 \cdot 91)$$

$$\gcd(39, 13)$$

$$91 = 39 \cdot 2 + 13$$

$$= -2 \cdot 221 + 5 \cdot 91$$

$$\gcd(13, 0)$$

$$39 = 13 \cdot 3 + 0$$

$$13$$

$$13 = -2 \cdot 221 + 5 \cdot 91$$

Problem 3 Inverses

Find an inverse of a modulo m for each of these pairs of relatively prime integers.

a. $a = 101, m = 4620$

b. $a = 144, m = 233$

Problem 3 Answer Key



First prove that $\gcd(4620, 101) = 1$

$\gcd(4620, 101) =$	
$\gcd(101, 75)$	$4620 = 101 \cdot 45 + 75$
$\gcd(75, 26)$	$101 = 75 \cdot 1 + 26 \checkmark$
$\gcd(26, 23)$	$75 = 26 \cdot 2 + 23 \checkmark$
$\gcd(23, 3)$	$26 = 23 \cdot 1 + 3 \checkmark$
$\gcd(3, 2)$	$23 = 3 \cdot 7 + 2 \checkmark$
$\gcd(2, 1)$	$3 = 2 \cdot 1 + 1 \checkmark$
$\gcd(1, 0)$	$2 = 1 \cdot 2 + 0 \checkmark$

Then use the pulverizer to find the linear combination

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3 \\ &= -1 \cdot 23 + 8(26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23 \\ &= 8 \cdot 26 - 9(75 - 2 \cdot 26) = -9 \cdot 75 + 26 \cdot 26 \\ &= -9 \cdot 75 + 26(101 - 1 \cdot 75) = 26 \cdot 101 - 35 \cdot 75 \\ &= 26 \cdot 101 - 35(4620 - 45 \cdot 101) = -35 \cdot 4620 + 1601 \cdot 101 \end{aligned}$$

Answer:

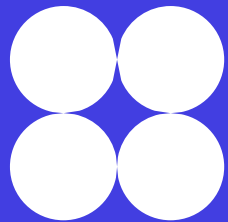
1601 is the inverse of 101 modulo 4620.

In other words

If $101d \equiv 1 \pmod{4620}$

Then $d = 1601$

*Follow the same format for part b: Answer 89



RACKET TIME