1.28 says we have an algorithm to replace any number modulo n with a number between 0 and $n-1$: Use the division alg. to divide a by n. Then a is cong. to its remainder.

Ex: $237 \equiv \underset{?}{\underline{6}} \pmod 7$

$$237 = q \cdot 7 + r \qquad 0 \le r \le 6$$
$$(0 \le r < 7)$$
$$= 33 \cdot 7 + 6$$

$7 \cdot 30 = 210$

$7 \cdot 31 = 217$

$7 \cdot 32 = 224$

$7 \cdot 33 = 231$

Ex: By Thm 1.18: $237^2 = 56{,}169$

$$56{,}169 \equiv 6^2 \pmod 7$$
$$\equiv 36 \pmod 7 \qquad 36 = 5 \cdot 7 + 1$$
$$\equiv 1 \pmod 7$$

Def: If a and b are integers

- a common divisor of a and b is an integer d such that $d \mid a$ and $d \mid b$.
- the greatest common divisor of a and b (if a and b are not both 0) is the largest number which is a common divisor of a and b.

Notation: gcd(a, b) or just (a, b).

1.31: (36, 22)

Divisors of 36

1, 2, 3, 4, 6, 9, 12, 18, 36

Divisors of 22

1, 2, 11, 22

$$36 = 1 \cdot 36 = 2 \cdot 18 = 3 \cdot 12 = 4 \cdot 9 = 6 \cdot 6$$

$$\boxed{(36, 22) = 2}$$

$$22 = 1 \cdot 22 = 2 \cdot 11$$

Next HW: 1.31 - 1.35

New Presentation sign-up