DIS 4A

# EUCLID'S ALGORITHM

**goal:** calculate $\gcd(x,y)$

**theorem:** $\gcd(x,y) = \gcd(y, x \bmod y)$, $x \geq y$

↳ we can iteratively reduce the numbers we are calculating the gcd for until one of them is zero.

↳ intuitively: a number $d$ divides $x$ and $y$

$$\Updownarrow$$

$d$ divides $y$ and the remainder when dividing $x$ by $y$

example: $\gcd(\underset{x}{10}, \underset{y}{6}) = \gcd(\underset{y}{6}, \underset{x \bmod y}{4})$

$\gcd(10, 6) = \gcd(6,4) = \gcd(4,2) = \gcd(2,0) = 2$

# EXTENDED EUCLID'S ALGORITHM

goal: in addition to calculating $\gcd(x, y)$,
find $a, b$ such that $\gcd(x, y) = ax + by$

how? q1 on the worksheet :)

note: when $\gcd(x, y) = 1$, we can solve for
the inverses $x^{-1} \pmod{y}$ and $y^{-1} \pmod{x}$

ex.

$$ax + by = 1 \pmod{y}$$

$$ax \equiv 1 \pmod{y}$$

$$x^{-1} \equiv a \pmod{y}$$

( and similarly for $y^{-1}$)

# CHINESE REMAINDER THEOREM

for coprime positive integers $n_1, n_2, \dots n_k$, there is a unique solution (mod $n_1 n_2 \dots n_k$) to the system of equations.

$$x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

$$\vdots$$

$$x \equiv a_k \pmod{n_k}$$

the solution:

don't memorize this! understand each of the terms (q2)

$$x = \left[ \sum_{i=1}^{k} a_i \left(\frac{N}{n_i}\right) \left( \left(\frac{N}{n_i}\right)^{-1} \bmod n_i \right) \right] \bmod N$$

where $N = n_1 n_2 \dots n_k$