$a = 54$, $b = 17$

Find $\gcd(a,b)$ using Euclid's alg:

$(u,v) \in \mathbb{Z} \times \mathbb{Z}$ s.t. $u \cdot a + v \cdot b = \gcd(a,b)$

→ All $(u,v) \in \mathbb{Z} \times \mathbb{Z}$ ——— // ———

$a = b \cdot q + r$

$54 = 17 \cdot 3 + 3$

$17 = 3 \cdot 5 + 2$

$3 = 2 \cdot 1 + 1$ → gcd

$2 = 1 \cdot 2 + 0$

$\gcd(54,17) = 1 = 3 - 2 =$

$= 3 - (17 - 3 \cdot 5) =$

$= 3 \cdot 6 - 17 =$

$= 6 \cdot (54 - 17 \cdot 3) - 17 =$

$= 6 \cdot 54 - 19 \cdot 17 = 1 \Rightarrow (u_0, v_0) = (6, -19)$

a b one solution

$$54 \cdot u + 17 \cdot v = 1$$

$$54 \cdot u_0 + 17 \cdot v_0 = 1$$

$$\Rightarrow$$

$$54(u - u_0) + 17(v - v_0) = 0$$

$$u - u_0 = \frac{-17(v - v_0)}{54} \in \mathbb{Z} \iff 54 \mid 17(v - v_0) \iff$$

$$\gcd(54, 17) = 1$$

$$\iff 54 \mid v - v_0 \iff v - v_0 = 54 \cdot k \; ; \; k \in \mathbb{Z}$$

$$u - u_0 = \frac{-17(54 \cdot k)}{54} = -17k$$

$$S = \{u = -17k + u_0, \; v = 54k + v_0 \mid k \in \mathbb{Z}\}$$

$(6, -19)$ $\quad k = 0$

$(-11, 35)$ $\quad k = 1$

$(-28, 89)$ $\quad k = 2$

$a = 128$, $b = 36$

Find $\gcd(a,b)$ using Euclid's alg:

$(u,v) \in \mathbb{Z} \times \mathbb{Z}$ s.t. $u \cdot a + v \cdot b = \gcd(a,b)$

$\rightarrow$ All $(u,v) \in \mathbb{Z} \times \mathbb{Z}$ ——— // ———

$128 = 36 \cdot 3 + 20$	$\gcd(128,36) = 4 =$
$36 = 20 \cdot 1 + 16$	$= 20 - 16 = 20 - (36 - 20) =$
$20 = 16 \cdot 1 + 4$	$= 2 \cdot 20 - 36 = 2 \cdot (128 - 3 \cdot 36) - 36 =$
$16 = 4 \cdot 4 + 0$	$= 2 \cdot 128 - 7 \cdot 36 = 4$
	$(u_0, v_0) = (2, -7)$
$4 = 3 \cdot 1 + 1$	

$u_0 \cdot 128 + v_0 \cdot 36 = 4$ ↶

$u \cdot 128 + v \cdot 36 = 0$ (−)

$128(u - u_0) + 36(v - v_0) = 0 \Leftrightarrow$

$\Leftrightarrow u - u_0 = \frac{-36 \cdot (v - v_0)}{128} = \frac{-9 \cdot (v - v_0)}{32} \in \mathbb{Z} \Leftrightarrow$

$$\left.\begin{array}{l} 32 \mid 9\cdot(v-v_0) \\ \gcd(32,9)=1 \end{array}\right\} \Leftrightarrow 32 \mid v-v_0 \Leftrightarrow$$

$$\Leftrightarrow v-v_0 = 32\cdot k \;;\; k\in\mathbb{Z} \Rightarrow$$

$$u-u_0 = \frac{-9\cdot 32\,k}{32} = -9k$$

$$S = \{v = 32k+v_0 \;;\; u=-9k+v_0 \mid k\in\mathbb{Z}\}$$

$$= \{v = 32k-7 \;,\; 2+9k \mid k\in\mathbb{Z}\}$$

- Find $\gcd(2^{128}-1, 2^{36}-1) = ?$

$$2^{128}-1 = (2^{36}-1)\cdot 2^{92} + (2^{92}-1)$$

$$2^{92}-1 = (2^{36}-1)\cdot 2^{56} + (2^{56}-1)$$

$$2^{56}-1 = (2^{36}-1)\cdot 2^{20} + (2^{20}-1)$$

$$2^{128}-1 = (2^{36}-1)\cdot(2^{92}+2^{56}+2^{20}) + (2^{20}-1)$$

$$2^{36}-1 = (2^{20}-1)\cdot 2^{16} + 2^{16} - 1$$

$$2^{20}-1 = (2^{16}-1)\cdot 2^{4} + 2^{4} - 1$$

$$2^{16}-1 = (2^{4}-1)\cdot(2^{12}+2^{8}+2^{4}+2^{0})$$

So $\gcd(2^{128}-1, 2^{36}-1) = 2^{4}-1$

HMW: $\gcd(a^{n}-1, a^{m}-1) = a^{\gcd(n,m)}-1$

$a \geq 2$
$n, m \in \mathbb{N}$

$$x^2 - 1 = (x-1)$$

$$(x^3-1) = (x-1)(x^2+x+1)$$

$$(x^n - a^n) = (x-a)(x^{n-1} + a x^{n-2} + \ldots + a^{n-1}) \; ; \forall n \geq 2$$

$$(x^n + a^n) = (x+a)(x^{n-1} - a x^{n-2} + a^2 x^{n-3} - \ldots + a^{n-1}) \; ; \; n \text{ odd}$$

HWK: Find $\gcd(70, 21, 18)$

and u, v, w s.th.

$70u + 21v + 18 \cdot w = \gcd(70, 21, 18)$

Prop: $r_{i+2} < \frac{1}{2} r_i$ whenever $r_{i+2} \neq 0$

$$a = b \cdot q_1 + r_1 \qquad 0 \leq r_1 \leq |b|$$

$$b = r_1 \cdot q_2 + r_2 \qquad 0 \leq r_2 \leq r_1$$

$$\vdots \qquad \vdots$$

$$r_i = r_{i+1} \cdot q_{i+2} + r_{i+2} \qquad 0 \leq r_{i+2} \leq r_{i+1}$$

Assume that $r_{i+2} \geq \frac{1}{2} r_i$

$$\Leftrightarrow 2 \cdot r_{i+2} \geq r_i$$

$$\Leftrightarrow 2 r_{i+2} \geq r_{i+1} \cdot q_{i+2} + r_{i+2}$$

$$\Leftrightarrow r_{i+2} \geq r_{i+1} \cdot q_{i+2} \Rightarrow$$

But $r_{i+2} < r_{i+1}$

$\Rightarrow q_{i+2} = 0 \Rightarrow r_i = r_{i+2}$ } False

$r_{i+2} < r_{i+1} < r_i$

Euler's totient function

$n \geq 2 \quad ; \quad n \in \mathbb{N}$

$\varphi(n) = |\{ 1 \leq x < n : \gcd(n, x) = 1 \}|$

Let $\varphi(1) = 1$

Examples $n = p$ prime $\varphi(p) = p - 1$

$k \geq 1 \quad \varphi(p^k) = |\{1, 2, 3, \dots, p^k\} \setminus \{\text{multiples of } p \text{ in } 1 \leq \dots \leq p^k\}|$

$p, 2 \cdot p, 3 \cdot p, \dots, p^k = p \cdot p^{k-1}$

$1 \leq x < p^k$

$\gcd(x, p^k) = 1 \iff$

$\iff \gcd(x, p) = 1 \iff x \nmid x$

$\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$

Then: If $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_t^{a_t}$ where

$p_1, p_2, \ldots, p_t$ distinct primes

$a_1, a_2, \ldots, a_t \geq 0$

Then: $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_t}\right)$

$1 \leq x \leq n$

$\gcd(x, n) = 1 \iff (p_1 \nmid x)$ or $(p_2 \nmid x)$ or $\ldots$ or $(p_t \nmid x)$

HWK

Use Incl. - Excl - Prime