i.e. $\exists m,n \in \mathbb{Z}$ s.t $21m + 27n = 3$

but there are not m', n' s.t. $21m' + 27n' = 2$ or 1.

Pf of Bezout: - Define $S = \{c \in \mathbb{N} \mid (\exists m,n \in \mathbb{Z})\ c = am+bn\}$

= set of positive linear combos of a, b.

- Observe: S is not empty since e.g. $|a| + |b| \in S$.
- Hence S has a least el'td by WOP.
- Fix $m,n \in \mathbb{Z}$ s.t. $d = am+bn$ (possible since $d \in S$).

WTS: $d = \gcd(a,b)$

Claim 1: ① $d \mid a$ and ② $d \mid b$

Pf: by division algorithm we can write $a = q \cdot d + r$ with $0 \leq r < d$ (WTS: $r = 0$)

$$\Rightarrow r = a - qd$$
$$= a - q(am+bn)$$
$$= (1-qm)a + (-qn)b$$

- hence r is a linear combo of a, b

- we know $r \geq 0$. If $r > 0$ then $r \in S$.
- but $r < d$, so if $r \in S$ would contradict minimality of d
- hence $r \notin S$, i.e. $r = 0$.

$\Rightarrow a = q \cdot d$ so $d \mid a$

② similarly can prove $d \mid b$.

Claim 2 d is greatest common divisor of a, b

Pf: - Sps $t \in \mathbb{N}$ and $t \mid a$ and $t \mid b$

- we prove $t \mid d$ which gives $t \leq d$.

$\exists k, \ell \in \mathbb{Z}$ s.t. $a = \ell t$ $b = kt$

So: $d = am + bn$

$= \ell t m + k t n$

$= t(\ell m + kn)$

$\Rightarrow t \mid d$

Claim 1 + Claim 2 proves theorem. ✓

Defn Fix $a,b \in \mathbb{Z}$. We say a,b are relatively prime iff $\gcd(a,b) = 1$

↳ It follows from Bezout: if a,b are relatively prime then $\exists\, m,n \in \mathbb{Z}$ s.t. $am+bn = 1$.

Ex's ① $\gcd(25,36) = 1$. So Bezout guarantees $\exists m,n \in \mathbb{Z}$ s.t. $25m + 36n = 1$.

And indeed: $25(-23) + 36(16) = 1$

② Observe: if p is prime then for any $a \in \mathbb{Z}$ either $p \mid a$ or $\gcd(a,p) = 1$

In particular if p,q are distinct primes then $\gcd(p,q) = 1$. Hence $\exists m,n$ s.t. $pm+qn = 1$ by Bezout.

e.g. if $p = 7$ $q = 31$ then

$$7(9) + 31(-2) = 1$$

Theorem (Euclid's Lemma)

Fix $a, b, c \in \mathbb{Z}$. If $a \mid bc$ and $\gcd(a,b) = 1$ then $a \mid c$.

Pf:- Sps $a \mid bc$ and $\gcd(a,b) = 1$

- then $\exists l \in \mathbb{Z}$ s.t. $bc = al$
- by Bezout, also $\exists m, n \in \mathbb{Z}$ s.t. $am + bn = 1$.

so:
$$\begin{aligned} c &= c \cdot 1 \\ &= c(am + bn) \\ &= acm + bcn \\ &= acm + aln \\ &= a(cm + ln) \end{aligned}$$

$\Rightarrow a \mid c$. ✓

of prop'n that follows immediately from thm.

Corollary: Fix $a, b \in \mathbb{Z}$ and $p \in \mathbb{N}$ a prime

If $p \mid ab$ then $p \mid a$ or $p \mid b$. (or both)

Pf:- If $p \mid a$, done. So assume $p \nmid a$.

- then $\gcd(p, a) = 1$
- Hence by Euclid: $p \mid b$.

Theorem (Fund. thm. of arithmetic)

Every $n \in \mathbb{N}$, $n > 1$, can be written uniquely (up to order of factors) as a product of primes.

Pf: Two parts: ① existence: every $n > 1$ can be written as a product of primes (proved already by strong induction) ✓

② uniqueness: HW

Ex's ① $21 = 3 \cdot 7 = 7 \cdot 3$ — no other way to factor into primes

$$21 \neq 2 \cdot 2 \cdot 5$$
$$\neq 2 \cdot 11$$

② $200 = 2 \cdot 100 = 2 \cdot 2 \cdot 50$
$= 2 \cdot 2 \cdot 2 \cdot 25$
$= 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5$
$= 2^3 \cdot 5^2$

③ $97 = 97$ (is prime)

We proved following theorem on day 1 — but implicitly used FTOA. Let's see complete proof now.

Thm (Euclid) There are infinitely many primes.

Pf: - Sps not, i.e. sps there are only finitely many primes, say $p_1, \dots, p_N$.

- Define $M = p_1 p_2 \cdots p_N + 1$
- By FTOA, M has a (unique) prime factorization, in particular, M is divisible by some prime p.
- must have $p \in \{p_1, p_2, \dots, p_N\}$ (these are the only primes, i.e. $p = p_j$ for some j $1 \le j \le N$.
- So: $M = p_j \cdot k$ for some $k \in \mathbb{N}$.
- But we knew $M = p_1 p_2 \cdots p_N + 1$

$$= p_j \underbrace{(p_1 p_2 \cdots p_{j-1} p_{j+1} \cdots p_N)}_{\text{call this } l} + 1$$

$$= p_j l + 1$$

Hence: $M = p_j k = p_j \ell + 1$

$\Rightarrow 1 = p_j k - p_j \ell = p_j (k - \ell)$

$\Rightarrow p_j \mid 1$, a contradiction as $p_j > 1$ (since p_j is prime) ✓

Note: proof actually shows that if $\{p_1, \ldots, p_N\}$ is any set of primes, the number $p_1 p_2 \cdots p_N + 1$ can only be divisible by primes $p \notin \{p_1, \ldots, p_N\}$

e.g. consider $\{3, 5, 7\}$

then: $3 \cdot 5 \cdot 7 + 1 = 106 = 2 \cdot 53$

no 3, 5, 7 in factors