**Last time:** Which $z = r^2 + s^2$?

$z = 0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, \ldots$ ?

Missing $z$'s: $3, 6, 7, 11, 12, 14, 15, 19, 21, 23, 27$

$2 \cdot 3$, $4 \cdot 3$, $2 \cdot 7$, $3 \cdot 5$, $3 \cdot 7$

**Lemma 1:** If $z \equiv 3 \bmod 4 \Rightarrow z \neq r^2 + s^2$,

**Def:** $a \equiv b \pmod c$ iff $c \mid (b-a)$ — $a$ & $b$ are in same residue class

**Ex:** $34 \pmod 5$, $27 \pmod 3$, $42 \pmod{11}$,

$4 \in [0,4]$ $\quad 0$ $\quad 9 \in [0,10]$.

**Lemma 2:** $a+b \pmod c \equiv a \pmod c + b \pmod c$.

$a \cdot b \pmod c \equiv a \pmod c \cdot b \pmod c$.

Ex: $5+7 \pmod 4$, $6\cdot 8 \pmod 3$, $9\cdot 10 \pmod 7$

$12 \equiv 0$ ; $1+3 \equiv 4 \equiv 0$. ; $48 \equiv 0$ ; $0\cdot 2 = 0$ ; $90 \equiv 6 \equiv 2\cdot 3$.

**Pf Lemma 2:** A representative for $a \pmod c$ is $a+c\cdot n$, rep for $b \pmod c$ is $b+c\cdot m$.

**Karen:** $a = c\cdot n + k$ & $b = c\cdot m + l$. So $a \equiv k \pmod c$, $b \equiv l \pmod c$.

$a+b \pmod c \equiv k+l \pmod c$.

**Another:** $a+b = c\cdot n + k + c\cdot m + l = k+l+c(n+m)$.

**Rebecca:** $c \mid a-k$ & $c \mid b-l \Rightarrow c \mid (a-k)+(b-l)$.

$(a+b)-(k+l)$.

Abstractly, $a \pmod c = a + c\cdot\mathbb{Z}$

$a \pmod c + b \pmod c = a + c\mathbb{Z} + b + c\mathbb{Z}$.

$= a+b+c\mathbb{Z} = a+b \pmod c$.

Eg: $1 \pmod 4 = 1$

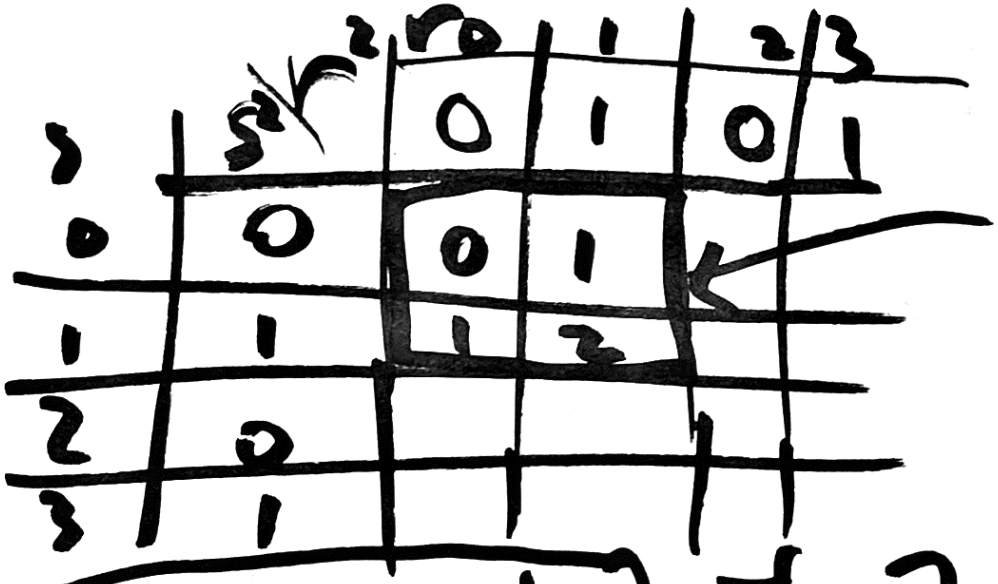
$a = k+n\cdot c$

$b = l+m\cdot c \Rightarrow a\cdot b = (k+n\cdot c)(l+m\cdot c) = R\cdot l + c(km + ln + nm)$

$c \mid a-k,\ c \mid b-l \Rightarrow c \mid (a\cdot b - k\cdot l)$

$\{\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\}$

**pf Lemma 1:** Look at $z = r^2+s^2 \pmod 4$




NO 3's. If $z \equiv 3(4)$

$\Rightarrow z \neq r^2+s^2\ (4)$.

**Key principle:** If $\exists$ solution $z = r^2+s^2$ in $\mathbb{Z}$,

$\Rightarrow \exists$ soln to $z \equiv r^2+s^2 \pmod 4$.

But if $z \equiv 3 \pmod 4$, then ↑ has no soln. So has no solution. "Local obstruction".

Maybe other obstructions?

**Exercise 1:** make a table for $r^2+s^2 \pmod 6$.

| $r^2$ \ $s^2$ | $0^2$ | $1^2$ | ... | $5^2$ |
|---|---|---|---|---|
| | | | | |

Any body missing?

**Exercise 2:** Take primes $<100$. Which are/aren't sums of 2 squares? (For Thu Fri)

More on modular arithmetic.

(mod 7): 5 ∈ powers of 5.

| n | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $5^n$ | 1 | 5 | 4 | 6 | 2 | 3 | 1 | 5 | 4 | |

| n | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $4^n$ | 4 | 2 | 1 | 4 | 2 | 1 | 4 | 2 ... |

(mod 7).

$a^{p-1} \bmod 7 \equiv 1.$

| n | 1 | 2 | 3 | 4 | 5 | 6 ← p−1 |
|---|---|---|---|---|---|---|
| $6^n$ | 6 | 1 | 6 | 1 | 6 | 1 |

---

**Fermat's Little Theorem:** If $a \not\equiv 0 \pmod{p}$, p prime

$$\boxed{a^{p-1} \equiv 1 \pmod{p}.}$$

Pf: key idea: look at $1 \cdot a, 2 \cdot a, 3 \cdot a, \ldots, (p-1)a$.

E.g.: $p=7$, $a=4$,

$1\cdot 4,\ 2\cdot 4,\ 3\cdot 4,\ 4\cdot 4,\ 5\cdot 4,\ 6\cdot 4.$

$\quad\ "\quad\ "\quad\ "\quad\ "\quad\ "\quad\ "$

$4,\ 1,\ 5,\ 2,\ 6,\ 3.$

**Claim:** $k\cdot a \equiv \ell\cdot a \Rightarrow k\equiv \ell$.

$\Leftrightarrow$

$p \mid k\cdot a - \ell\cdot a \iff p \mid a(k-\ell) \Rightarrow p \mid (k-\ell)$.

So $1\cdot a, 2\cdot a, \dots, (p-1)\cdot a$ all distinct, nonzero (mod $p$).

& there are $(p-1)$ numbers $\Rightarrow$ all numbers $1, 2, \dots, p-1$ in some permuted order.

So $\underbrace{1\cdot a\cdot 2\cdot a\cdot 3\cdot a\cdots(p-1)\cdot a}_{(p-1)!\cdot a^{p-1}} \equiv \underbrace{1\cdot 2\cdot 3\cdots(p-1)}_{(p-1)!} \pmod p$

so $p \mid \underbrace{[(p-1)!\, a^{p-1} - (p-1)!]}_{(p-1)!\,[a^{p-1} - \square}$ . $\Rightarrow p \mid (a^{p-1} - 1)$

. $\Rightarrow a^{p-1} \equiv 1 \ (p)$.

---