Scaletta per una lezione di Teoria dei Numeri, stage junior di Pavia 2005

- Intro, captatio benevolentiae. Prendere appunti + voglio che facciano domande.

- Lavoriamo con i numeri interi. Variabili intere. Comodità: fattorizzazione, divisibilità.
- **Es:** Diofanteina che si fa fattorizzando: (Bocconata) trovare p t.c. $5p + 49 = \square$. Achtung, modi diversi di spezzare. Rmk $p \mid ab \Rightarrow \ldots$
- Simbolo $|$. **Es:** $3 \mid 18$. Simile a $\leq$: $3 \mid 6, 6 \mid 18 \Rightarrow 3 \mid 18$. Domanda: $a \mid b$, $b \mid a \Rightarrow ?$
- $3 \mid a$, $3 \mid b \Rightarrow 3 \mid a + b$. Possiamo aggiungere/sottrarre multipli del divisore. **Es:** criterio divisibilità per 4.
- Se $d \mid$ due termini in $a + b = c$, allora divide anche il terzo. **Es:** $3x^2 - 2y^2 = 1998$, un po' di lavoro.

- mcd: **Es:** $\text{mcd}(27, 90) = 9$. Possiamo aggiungere multipli "dell'altro numero". **Es:** $\text{mcd}(91, 196) = \text{mcd}(91, 196 - 2 \cdot 91) = \text{mcd}(91, 14) = \text{mcd}(14, 91) = \text{mcd}(14, 91 - 14 \cdot 6) = \text{mcd}(14, 7) = 7$
- funziona sempre: enunciato divisione euclidea
- divisibilità si usa anche "a rovescio": se voglio $\text{mcd}(78, 385)$ e trovo due numeri t.c. $78a - 385b = 1$, allora mcd = 1. Il fatto si inverte (claima Bézout)

Congruenze:

- Esempio di prova del 9: $122 \cdot 57 = 6954$. Cambiare una cifra del risultato
- "Sporcarsi le mani": prova a calcolare i residui dei numeri più bassi. Congettura: residuo=resto della divisione per 9.
- resto(ab)=resto(a)·resto(b), e così somma. È un fatto generale: notazione di Gauss (con le tre definizioni, stesso resto, $m \mid a - b$,$a = b + km$).
- Le congruenze si sommano, sottraggono, moltiplicano. Dire quando si può "semplificare".
- Esempi di calcolo di resti, XXX.

- Riconosci come congruenze: calcoli di parità (P·D=P), ultima cifra.
- Possiamo dimostrare la congettura, residuo da somma cifre=resto div. per 9.
- **Es:** fine di $3x^2 - 2y^2 = 1998$.
- inversi. Esistono sempre. **Es:** congruenze lineari $ax \equiv b$: $5x \equiv 6 \mod 7$

- Potenze e congruenze:
- Potenze con la stessa base. Sono tutte periodiche. Claim piccolo teo. Fmt. [dim. coi sistemi di residui se c'è tempo. XXX: o con le perline?]. Dire en passant che si generalizza.
- Potenze con lo stesso esponente: i residui quadratici sono la metà, perché?. Accenni a cosa succede

---

- teo. cinese: smontare e rimontare congruenze, esempio $x \equiv 4 \mod 5$, $x \equiv 1 \mod 7 \Leftrightarrow x \equiv 29 \mod 35$.
- se c'è tempo: giustificazione intuitiva
- Estensione a n equazioni. Tutti i sistemi si risolvono.
- **Es:** esistono n numeri composti consecutivi: uno multiplo di 2, uno di 3, uno di 5, eccetera.

- Extras: formula per il numero e la somma dei divisori di un intero.