

C1: *Show no work.*

a The author of our text is Circle: **DNE Euler Fermat Waldo Pollard Fuchs Gauss Archimedes Silverman Sanders Shannon Strayer Tony Tori**

b The smallest natnum which is *not* a sum of three squares is .

c A primitive Pythagorean triple has $28^2 + b^2 = c^2$, where $b = \text{_____}$ and $c = \text{_____}$ with $b \perp c$.

d Let $g := \sigma^{\otimes -1}$ [i.e., the convol-inverse of the divisor-sum fnc]. So $g(2) = \text{_____}$, $g(9) = \text{_____}$ and $g(18) = \text{_____}$.

e Let $f(x) := x^2 - 4x - 2$, and $Z_1 := t_0 := 3$. Note $f(Z_1) \equiv_5 0$. Note $f'(Z_1) = \text{_____} \not\equiv_5 0$. Use Hensel's lemma to compute coefficients $t_k \in [0..5)$ [put them in the blanks, below]

$$Z_4 = \underbrace{t_0 \cdot 5^0 + \text{_____} \cdot 5^1 + \text{_____} \cdot 5^2 + \text{_____} \cdot 5^3}_{Z_3}$$

so that *natnums* $Z_k := \sum_{i \in [0..k)} t_i 5^i$ satisfy

$$f(Z_k) \equiv 0 \pmod{5^k}, \quad \text{for } k = 2, 3, 4.$$

f With $A := 23$, $B := 20$, $U := A \cdot B = 460$, let \mathbf{J} be $(-230..230)$. There is a ring-iso $F: \mathbb{Z}_A \times \mathbb{Z}_B \rightarrow \mathbb{Z}_U$ sending (α, β) to $\langle G\alpha + H\beta \rangle_U$, using magic numbers

$G = \text{_____} \in \mathbf{J}$ and $H = \text{_____} \in \mathbf{J}$. A

mod- U root of poly $h(x) := 20 \cdot [x + 10]^3 + 23 \cdot [x - 2]$ is $(\text{_____}, \text{_____}) \xrightarrow{F} \text{_____} \in \mathbf{J}$.

g With $M := 22$ and $J := [0..M)$, use *repeated-squaring* to compute $6^{2048} \equiv_M \text{_____} \in J$. Since 2053 equals $2^{11} + 2^2 + 2^0$, the power $6^{2053} \equiv_M \text{_____} \in J$. [Hint: Compute with symm. residues, and use periodicity.]

OYOP: *In grammatical English sentences, write your essays on every **third** line (usually), so that I can easily write between the lines. Do **not** restate the question. Start each essay on a **new** sheet of paper.*

C2: Prove: *If $P \equiv_4 1$ and P is prime, then there exist integers x, y with $x^2 + y^2 = P$.* [If you use melding, then give a formula for it. You may use LST without proof.]

C3: For natnums n , define

$$S_n := 13^n + 17^n + 28^n + 31^n.$$

Prove, for *odd* posints n , that S_n is composite. [Hint: Look at $S_n \pmod{\text{something}}$.]

End of Class-C

C1: ___ ___ 165pts

C2: ___ ___ 85pts

C3: ___ ___ 55pts

Total: ___ ___ 305pts

Folks, I have had a great time learning Number Theory with you, this Summer. Stop by in future semesters to "Talk Math".

Cheers, Prof. Erroneous Monk