Test—7:30–8:50 am, April 7, 2025

Instructions: Answer all questions in the space provided Closed book; however, a 'cheat sheet' (one $8\frac{1}{2}$" $\times$ 11" sheet with your own handwriting) and a calculator are permitted. Cell phones and other aids are not permitted; in particular, cell phones may not be used as calculators. Time allowed: 80 minutes. Total value of questions: 100 points (plus 19 bonus points).

1. *(16 points)* Given integers a, b satisfying $a^2 + b^2 = n$, find two integers u, v such that $61n = u^2 + v^2$.

2. *(24 points)* (a) Compute $d = gcd(402, 147)$ and find integers r, s such that $d = 402r + 147s$.

(b) Show that the solution for r, s in (a) is not unique, by finding a *different* pair of integers (r, s) that also satisfies the required condition.

(c) The nation of Politzania uses currency based on the US dollar, but only two denominations of banknotes are used: the *grot*, each worth \$402; and the *klin*, each worth \$147. What is the smallest cash purchase that can be made in Politzania? and how is it possible (by the exchange of grots and klins) to achieve this minimum possible purchase?

3. *(18 points)* Fill in the blanks in the proof of the theorem below, using words taken from the following list. Some entries from the list may be used more than once, or not at all.

all	proof	lemma	integer	multiple	divisor	algorithm
some	equal	suppose	integers	multiplied	divisible	contradicts
hence	equals	formula	conclude	required	divides	contradiction

Theorem. Let a, b be integers, not both zero, and let d be the greatest common divisor of a and b. Let g be any integer. Then g is divisible by d, if and only if there exist $r, s \in \mathbb{Z}$ such that $g = ra + sb$.

Proof. Let $d = \gcd(a, b)$. By Euclid's _____, we have $d = xa + yb$ for _____ x, y. Now we prove the statement of the Theorem, beginning with the forward direction.

Assuming g is _____ by d, then $g = cd$ for _____ integer c. In this case, $g = (cx)a + (cy)b$, as _____.

Conversely, _____ $g = ra + sb$ for _____ $r, s \in \mathbb{Z}$. Since d divides a and b, it also _____ $ra + sb = g$. This completes the _____.

4. *(16 points)* Let $p = 1234567$, $r = 917831$. You are given that $4^{p-1} \equiv r \mod p$, and $4^{r-1} \equiv 1 \mod r$. *Based on this information only,* can you conclude

   (a) whether or not p is prime? Explain.

   (b) whether or not r is prime? Explain.

   Name any theorems used to justify your conclusions.

5. *(15 points)* Given an odd prime p, find a Pythagorean triple containing the number p.

6. *(30 points)* Answer TRUE or FALSE to each of the following statements.

(a) Every integer $n \geqslant 2$ factors as a product of primes, in an essentially unique way. _____*(True/False)*

(b) The integer 1200 is contained in infinitely many Pythagorean triples. _____*(True/False)*

(c) Euclid proved that there are infinitely many primes. _____*(True/False)*

(d) The equation $x^2 - 17y^2 = 1$ has infinitely many integer solutions. _____*(True/False)*

(e) The equation $x^3 + y^3 = z^3$ has no solutions in positive integers. _____*(True/False)*

(f) Given an arbitrary Diophantine equation, methods from the 20th century provide an algorithm which effectively answers the question of whether the equation has any integer solutions. _____*(True/False)*

(g) Given large integers m and n (each of which is hundreds of decimal digits long), it is generally impossible to determine whether or not m and n are relatively prime, unless we know the prime factorizations of m and n. _____*(True/False)*

(h) Typical computers using commonly available software are currently able to factor arbitrary integers having about 1000 digits. _____*(True/False)*

(i) Euler's totient function ϕ satisfies $\phi(2400) = \phi(24)\phi(100)$. _____*(True/False)*

(j) There is a unique integer $x \in \{1, 2, \ldots, 10^6\}$ satisfying $x \equiv 26 \mod 2^6$ and $x \equiv 3917 \mod 5^6$. _____*(True/False)*