Instructions. Answer each of the questions on your own paper, and be sure to show your work, including giving reasons, so that partial credit can be determined. Put your name on each page of your paper. There is a total possible of 70 points.

Here is a table of the indices to base 2 modulo 11. It may be useful for some problems.

a	1	2	3	4	5	6	7	8	9	10
$\operatorname{ind}_2 a$	0	1	8	2	4	9	7	3	6	5

---

1. [**12 Points**]

   (a) If x, y, z is a primitive Pythagorean triple with x even, then

   $$x = \underline{\hspace{3cm}}, \qquad y = \underline{\hspace{3cm}}, \qquad z = \underline{\hspace{3cm}},$$

   for some relatively prime positive integers s, t, not both odd, with $s < t$.

   (b) Find all of the right-angles triangles with relatively prime integer sides and base length $x = 20$.

   (c) Find all of the right-angles triangles with relatively prime integer sides and base length $y = 13$.

2. [**12 Points**]

   (a) Suppose that $(a, m) = 1$. Define $\operatorname{ord}_m a$, the order of a modulo m.

   (b) Suppose that $(a, 23) = 1$. What does Fermat's Little Theorem tell you about $\operatorname{ord}_{23} a$?

   (c) Find $\operatorname{ord}_{23} 3$.

3. [**12 Points**] Solve the following congruences. The table of indices modulo 11 may be useful.

   (a) $3x^4 \equiv 5 \pmod{11}$.

   (b) $x^8 \equiv 10 \pmod{11}$.

4. [**6 Points**] You have decided to do RSA cryptography with modulus $n = 19 \cdot 29$ and enciphering exponent $e = 5$. Calculate a deciphering exponent d.

5. [**12 Points**]

   (a) Prove that if n is a positive integer such that $n \equiv 3 \pmod 4$, then n cannot be written as a sum of two squares.

   (b) Find an example of a positive integer n such that $n \equiv 1 \pmod 4$, but n cannot be written as a sum of two squares.

6. [**6 Points**] Express $377 = 29 \cdot 13$ as a sum of two squares.

7. [**10 Points**] Define $F(n) = \sum_{d|n} \mu^2(d)\phi(d)$ where μ is the Möbius function and ϕ is the Euler-ϕ function. You may assume that μ and ϕ are multiplicative functions.

   (a) If p is a prime, then compute $F(p^k)$.

   (b) Evaluate $F(700)$.