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

$$x = \boxed{2st}, \qquad y = \boxed{t^2 - s^2}. \qquad z = \boxed{t^2 + s^2},$$

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 $x = 20$.

▶ **Solution.** $x = 20 = 2st$ so $st = 10$. Hence there are two choices for s and t:
Case 1: $s = 1$, $t = 10$. In this case $y = t^2 - s^2 = 100 - 1 = 99$ and $z = t^2 + s^2 = 100 + 1 = 101$. Thus, $(x, y, z) = (20, 99, 101)$ in this case.
Case 2: $s = 2$, $t = 5$. In this case $y = t^2 - s^2 = 25 - 4 = 21$ and $z = t^2 + s^2 = 25 + 4 = 29$. Thus, $(x, y, z) = (20, 21, 29)$ in this case. ◀

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

▶ **Solution.** $y = 13 = t^{-}s^2 = (t + s)(t - s)$. The only factorization of 13 is $1 \cdot 13$ so we get $t + s = 13$ and $t - s = 1$. Solving these two for t and s gives $t = 7$ and $s = 6$. Thus, $x = 2st = 2 \cdot 6 \cdot 7 = 84$ and $z = t^2 + s^2 = 49 + 36 = 85$. Hence, $(x, y, z) = (84, 13, 85)$ in this case. ◀

2. [**12 Points**]

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

▶ **Solution.** $\operatorname{ord}_m a$ is the smallest positive integer k such that $a^k \equiv 1 \pmod{m}$. ◀

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

▶ **Solution.** By Fermat's theorem, $a^{22} \equiv 1 \pmod{23}$. Since $a^h \equiv 1 \pmod{m}$ if and only if $h \mid \operatorname{ord}_m a$, it follows in this case that $\operatorname{ord} 23a \mid 22$, so that $\operatorname{ord}_{23} a$ must be 1, 2, 11, or 22. ◀

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

▶ **Solution.** Compute the powers of 3 modulo 23: $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 27 \equiv 4$, $3^4 \equiv 3 \cdot 4 \equiv 12$, $38 \equiv 12^2 \equiv 144 \equiv 6$, $3^{11} = 3^{8+3} = 3^8 3^3 \equiv 6 \cdot 4 \equiv 24 \equiv 1$. Thus, $311 \equiv 1 \pmod{23}$ but $3 /\!\!\equiv 1$ and $32 \not\equiv 1$. Thus, $ord_{23}a = 11$. ◀

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

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

   ▶ **Solution.** Applying ind_2 to the equation gives $\operatorname{ind}_2 3 + 4 \operatorname{ind}_2 x \equiv \operatorname{ind}_2 5 \pmod{10}$. From the index table: $\operatorname{ind}_2 3 = 8$ and $\operatorname{ind}_2 5 = 4$ so the linear congruence for $\operatorname{ind}_2 x$ becomes

   $$8 + 4 \operatorname*{ind}_2 x \equiv 4 \pmod{10}.$$

   Subtracting 8 gives $4 \operatorname{ind}_2 x \equiv -4 \pmod{10}$. Since $(4, 10) = 2$ and $2 \mid -4$ it follows that there are two non-congruent solutions to this linear congruence. One is clearly $ind_2 x \equiv -1 \equiv 9 \pmod{10}$, and then the other is $\operatorname{ind}_2 x \equiv 9 + \frac{10}{2} \equiv 9 + 5 \equiv 4 \pmod{10}$. Now, $\operatorname{ind}_2 x \equiv 9 \pmod{10}$ gives $x \equiv 6 \pmod{11}$ and $\operatorname{ind}_2 x \equiv 4 \pmod{10}$ gives $x \equiv 5 \pmod{11}$ from the index table. Thus, the non-congruent solutions are $x \equiv 5,\ 6 \pmod{11}$. ◀

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

   ▶ **Solution.** Applying ind_2 to the equation gives a linear congruence $8 \operatorname{ind}_2 x \equiv \operatorname{ind}_2 10 \pmod{10}$. From the index table, this becomes

   $$8 \operatorname*{ind}_2 x \equiv 5 \pmod{10}.$$

   Since $(8, 10) = 2$ and $2 \nmid 5$ this linear congruence has no solutions, and hence the original congruence also has no solutions. ◀

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.

▶ **Solution.** $\phi(n) = \phi(19 \cdot 29) = \phi(19)\phi(29) = 18 \cdot 28 = 504$. Then e and d are related by $ed \equiv 1 \pmod{\phi(n)}$ which in this case is $5d \equiv 1 \pmod{504}$. Solving this linear congruence by the Euclidean algorithm gives $d \equiv 101 \pmod{504}$. ◀

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.

   ▶ **Solution.** If a is an integer then $a \equiv 0,\ 1,\ 2,\ 3 \pmod 4$, Then $a^2 \equiv 0$ or 1 modulo 4. Hence, if $n = a^2 + b^2$ where a and b are integers, then $n \equiv 0 + 0 = 0$, $0 + 1 = 1$, or $1 + 1 = 2$ modulo 4. Hence, if $n \equiv 3 \pmod 4$, then n cannot be 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.

▶ **Solution.** $21 = 3 \cdot 7$ is not a sum of two squares since a prime congruent to 3 modulo 4 (namely 3 or 7) appears in the prime factorization to an odd power. However, $21 \equiv 1 \pmod 4$. ◀

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

▶ **Solution.** $377 = 13 \cdot 29 = (2^2 + 3^2)(2^2 + 5^2) = (2 \cdot 2 + 3 \cdot 5)^2 + (2 \cdot 5 - 3 \cdot 2)^{=} 19^2 + 4^2$. ◀

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 $F(p^k)$.

▶ **Solution.**

$$\begin{aligned} F(p^k) &= \sum_{d|p^k} \mu^2(d)\phi(d) \\ &= \mu^2(1)\phi(1) + \mu^2(p) + \mu^2(p^2)\phi(p^2) + \cdots + \mu^2(p^k)\phi(p^k) \\ &= 1^2 \cdot 1 + (-1)^2(p-1) + 0^2 \cdot \phi(p^2) + \cdots + 0^2 \cdot \phi(p^k) \\ &= 1 + (p-1) \\ &= p. \end{aligned}$$

◀

(b) Evaluate $F(700)$.

▶ **Solution.** Since μ and ϕ are multiplicative functions, so is F. Then,

$$F(700) = F(2^2 \cdot 5^2 \cdot 7) = F(2^2)F(5^2)F(7) = 2 \cdot 5 \cdot 7 = 70.$$

◀