1. (a) Compute $\varphi(m)$ for $m = 9$, $m = 25$, and $m = 49$ using the following brute-force method. Write down a list of all the integers from 1 to m (inclusive), and then cross out all the integers that aren't relatively prime to m.

Solution: For $m = 9$, we have

$$1 \quad 2 \quad \cancel{3} \quad 4 \quad 5 \quad \cancel{6} \quad 7 \quad 8 \quad \cancel{9}$$

so that $\varphi(9) = 9 - 3 = 6$.

For $m = 25$, we have

$$\begin{array}{rrrrr} 1 & 2 & 3 & 4 & \cancel{5} \\ 6 & 7 & 8 & 9 & \cancel{10} \\ 11 & 12 & 13 & 14 & \cancel{15} \\ 16 & 17 & 18 & 19 & \cancel{20} \\ 21 & 22 & 23 & 24 & \cancel{25} \end{array}$$

so that $\varphi(25) = 25 - 5 = 20$.

For $m = 49$, we have

$$\begin{array}{rrrrrrr} 1 & 2 & 3 & 4 & 5 & 6 & \cancel{7} \\ 8 & 9 & 10 & 11 & 12 & 13 & \cancel{14} \\ 15 & 16 & 17 & 18 & 19 & 20 & \cancel{21} \\ 22 & 23 & 24 & 25 & 26 & 27 & \cancel{28} \\ 29 & 30 & 31 & 32 & 33 & 34 & \cancel{35} \\ 36 & 37 & 38 & 39 & 40 & 41 & \cancel{42} \\ 43 & 44 & 45 & 46 & 47 & 48 & \cancel{49} \end{array}$$

so that $\varphi(49) = 49 - 7 = 42$.

(b) Make a conjecture about the value of $\varphi(p^2)$ when p is a prime. Explain why you think your conjecture is true.

Solution: We conjecture that $\varphi(p^2) = p^2 - p$. There are p^2 integers n satisfying $1 \leq n \leq p^2$. Of these numbers, the only ones not relatively prime to p^2 are the multiples of p, and there are exactly $p^2/p = p$ such multiples.

2. (a) Using the same method as in Problem 1a, find $\varphi(m)$ for $m = 15$, $m = 21$, and $m = 35$.

Solution: For $m = 15$, we'll cross out all the multiples of 3 with forward slashes and all the multiples of 5 with backslashes. We get

$$\begin{array}{ccccc} 1 & 2 & \not{3} & 4 & \not{5} \\ \not{6} & 7 & 8 & \not{9} & \not{10} \\ 11 & \not{12} & 13 & 14 & \not{15} \end{array}$$

so that $\varphi(15) = 15 - 5 - 3 + 1 = 8$.

For $m = 21$, we'll cross out all the multiples of 3 with forward slashes and all the multiples of 7 with backslashes. We get

$$\begin{array}{ccccccc} 1 & 2 & \not{3} & 4 & 5 & \not{6} & \not{7} \\ 8 & \not{9} & 10 & 11 & \not{12} & 13 & \not{14} \\ \not{15} & 16 & 17 & \not{18} & 19 & 20 & \not{21} \end{array}$$

so that $\varphi(21) = 21 - 7 - 3 + 1 = 12$.

For $m = 35$, we'll cross out all the multiples of 5 with forward slashes and all the multiples of 7 with backslashes. We get

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & \not{5} & 6 & \not{7} \\ 8 & 9 & \not{10} & 11 & 12 & 13 & \not{14} \\ \not{15} & 16 & 17 & 18 & 19 & \not{20} & \not{21} \\ 22 & 23 & 24 & \not{25} & 26 & 27 & \not{28} \\ 29 & \not{30} & 31 & 32 & 33 & 34 & \not{35} \end{array}$$

so that $\varphi(35) = 35 - 7 - 5 + 1 = 24$.

(b) Make a conjecture about the value of $\varphi(pq)$ where p and q are primes with $p \neq q$. Explain why you think your conjecture is true.

Solution: We conjecture that $\varphi(pq) = pq - p - q + 1$. In each case, we started with pq integers, then crossed out p of them (the multiples of q) and then q of them (the multiples of p). In each case, there was one number, pq itself, that was crossed out twice, so the number of crossings-out was $p + q - 1$.

3. The number 1013 is a prime.

(a) Using no computing power beyond a standard hand-held calculator, find $\overline{234}$ modulo 1013 (expressed as an integer between 1 and 1012 inclusive). Assume that your calculator maintains only eight digits of precision, and explain how you can work around this limitation.

Solution: By Fermat's theorem, we know that $234^{1012} \equiv 1 \pmod{1013}$, so the multiplicative inverse of 234 is simply 234^{1011}. Decomposing the exponent 1011 in base 2, we get

$$1011 = 512 + 256 + 128 + 64 + 32 + 16 + 2 + 1,$$

so we'll need to find representatives of the residue classes 234^{2^n} up through $2^n = 512$. By succesive squaring and reducing modulo 1013, we produce the following table:

$$\begin{aligned}
234^1 &\equiv 234 \pmod{1013} \\
234^2 &\equiv 54 \pmod{1013} \\
234^4 &\equiv 890 \pmod{1013} \\
234^8 &\equiv 947 \pmod{1013} \\
234^{16} &\equiv 304 \pmod{1013} \\
234^{32} &\equiv 233 \pmod{1013} \\
234^{64} &\equiv 600 \pmod{1013} \\
234^{128} &\equiv 385 \pmod{1013} \\
234^{256} &\equiv 327 \pmod{1013} \\
234^{512} &\equiv 564 \pmod{1013}
\end{aligned}$$

Thus we get

$$\begin{aligned}
234^{1011} &\equiv 234^{512} \times 234^{256} \times 234^{128} \times 234^{64} \\
&\quad \times 234^{32} \times 234^{16} \times 234^{2} \times 234^{1} \pmod{1013} \\
&\equiv 564 \times 327 \times 385 \times 600 \times 233 \times 304 \times 43 \times 234 \pmod{1013}
\end{aligned}$$

Now we need to exercise a little care, because the product in the previous line will have about 20 digits, so if we multiply it out all at once, we may lose some accuracy. To avoid this trap, we multiply the numbers together two at a time, and reduce modulo 1013 as we go. We get

$$\begin{aligned}
564 \times 327 &\equiv 62 \pmod{1013} \\
62 \times 385 &\equiv 571 \pmod{1013} \\
571 \times 600 &\equiv 206 \pmod{1013} \\
206 \times 233 &\equiv 387 \pmod{1013} \\
387 \times 304 &\equiv 140 \pmod{1013} \\
140 \times 54 &\equiv 469 \pmod{1013} \\
469 \times 234 &\equiv 342 \pmod{1013}
\end{aligned}$$

The answer is 342.

(b) Solve the linear congruence $234x + 567 \equiv 251 \pmod{1013}$.
Solution: We add $1013 - 567$ to each side of the congruence to get

$$234x \equiv 697 \pmod{1013}.$$

Next we multiply each side by $\overline{234} \equiv 342$ and reduce modulo 1013. We get

$$\begin{aligned} x &\equiv 342 \times 697 \pmod{1013} \\ &\equiv 319 \pmod{1013} \end{aligned}$$

4. The number 667 is the product of the two primes 23 and 29.

(a) Find $\overline{67}$ modulo 667 (expressed as an integer between 1 and 666 inclusive).
Solution: By our conjecture above, $\varphi(667) = 667 - 23 - 29 + 1 = 616$. Thus by Euler's generalization of Fermat's theorem, we know that

$$67^{616} \equiv 1 \pmod{667}$$

and thus that $\overline{67} \equiv 67^{615} \pmod{667}$.

Expanding 615 in base 2, we get

$$615 = 512 + 64 + 32 + 4 + 2 + 1$$

so we'll need the values of 67^{2^n} up through $2^n = 512$. By repeated squarings and reductions modulo 667, we construct the table

$$\begin{aligned} 67^1 &\equiv 67 \pmod{667} \\ 67^2 &\equiv 487 \pmod{667} \\ 67^4 &\equiv 384 \pmod{667} \\ 67^8 &\equiv 49 \pmod{667} \\ 67^{16} &\equiv 400 \pmod{667} \\ 67^{32} &\equiv 587 \pmod{667} \\ 67^{64} &\equiv 397 \pmod{667} \\ 67^{128} &\equiv 197 \pmod{667} \\ 67^{256} &\equiv 123 \pmod{667} \\ 67^{512} &\equiv 455 \pmod{667} \end{aligned}$$

Thus we have

$$\begin{aligned} 67^{615} &\equiv 67^1 \times 67^2 \times 67^4 \times 67^{32} \times 67^{64} \times 67^{512} \pmod{667} \\ &\equiv 67 \times 487 \times 384 \times 587 \times 397 \times 455 \pmod{667} \\ &\equiv 448 \pmod{667}. \end{aligned}$$

(b) What happens when you use the same technique to try to find $\overline{46}$ modulo 667?

Solution: Since 46 is not relatively prime to 667, we suspect something may go wrong. In fact, we know something must go wrong, because Theorem 2.9 says that 46 can't have a multiplicative inverse modulo 667.

If we nonetheless blindly try to compute 46^{615}, we notice a curious phenomenon:

$$46^{2^n} \equiv 552 \pmod{667}$$

for all $n \geq 2$. Upon closer inspection, we determine that

$$\begin{aligned} 46^1 &\equiv 46 \pmod{667} \\ 46^2 &\equiv 115 \pmod{667} \\ 46^3 &\equiv 621 \pmod{667} \\ 46^4 &\equiv 552 \pmod{667} \\ 46^5 &\equiv 46 \pmod{667} \end{aligned}$$

and then the sequence repeats. This makes it clear where all those 552's are coming from: if n is a multiple of 4, then we'll get

$$46^n \equiv 552 \pmod{667}.$$

It also makes it clear why this technique will fail to find a multiplicative inverse: every power of 46 (beyond the zeroth power) is congruent to either 46, 115, 621, or 552. In particular, no positive power of 46 can be 1, so no power of 46 can be congruent to $\overline{46}$.

5. (a) Find two solutions to the congruence $x^2 + 1 \equiv 0 \pmod{1013}$. Recall that 1013 is prime. Your solutions should not be congruent to one another modulo 1013. Please do not try to do this problem by brute force.

HINT: First show that any x satisfying the given congruence also satisfies $x^4 \equiv 1 \pmod{1013}$. Fermat's theorem will then tell you where to look for solutions.

Solution: If $x^2 + 1 \equiv 0 \pmod{1013}$, then $x^2 \equiv -1 \pmod{1013}$. We may square both sides of this congruence to conclude that $x^4 \equiv 1 \pmod{1013}$.

So we're looking for a fourth root of 1. By Fermat's theorem, we know that

$$a^{1012} \equiv 1 \pmod{1013}$$

for any number a such that $1013 \nmid a$. The number 1012 happens to be divisible by 4, so we can write

$$a^{1012} \equiv (a^{253})^4 \equiv 1 \pmod{1013}$$

to see that any a (with $1013 \nmid a$) raised to the power 253 will be a fourth root of 1 modulo 1013. Using the computational tools that are now quite familiar to us, we find that

$$2^{253} \equiv 45 \pmod{1013} \quad \text{and} \quad 3^{253} \equiv 968 \pmod{1013}$$

We check that

$$45^2 + 1 = 2026 \equiv 0 \pmod{1013}$$

and that

$$968^2 + 1 = 937025 \equiv 0 \pmod{1013}.$$

Since we were asked for only two solutions, we can stop here: the answers are 45 and 968.

(b) Prove the following: Let p be a prime. If x and y are integers such that $x^2 \equiv y^2 \pmod{p}$, then either $x \equiv y \pmod{p}$ or $x \equiv -y \pmod{p}$.

Use this result to explain why the solutions you found in Problem 5a are the only solutions to $x^2 \equiv 1 \pmod{1013}$. (That is, any other solution must be congruent to one of your solutions modulo 1013.)

Solution: Suppose x and y are integers and that $x^2 \equiv y^2 \pmod{p}$. Then by definition of congruence, we have

$$p|(x^2 - y^2).$$

We factor the difference of two perfect squares to get

$$p|(x - y)(x + y).$$

Since p is a prime, we know (by Theorem 1.15) that either $p|(x - y)$ or $p|(x + y)$. If $p|(x - y)$, then $x \equiv y \pmod{p}$. If $p|(x + y)$, then we get $x + y \equiv 0 \pmod{p}$, which implies that $x \equiv -y \pmod{p}$. ∎

Now suppose that z is any solution to the congruence $x^2 + 1 \equiv 0 \pmod{1013}$.

Then $z^2 \equiv -1 \pmod{1013}$. But we also know that $45^2 \equiv -1 \pmod{1013}$. By Theorem 2.1(2), we can conclude that

$$z^2 \equiv 45^2 \pmod{1013}.$$

By the theorem we just proved, we may then conclude that either $z \equiv 45 \pmod{1013}$ or $z \equiv -45 \pmod{1013}$. Since $-45 \equiv 968 \pmod{1013}$, we have shown, as required, that z is congruent to either 45 or 968 modulo 1013. That is, we have found all the square roots of minus one.