TEST 1

JASON MEDCOFF

1. Given that if $n = 31864033$, then $24779170^2 \equiv 1 \mod n$, find a factor of n. Explain why this works.

Solution. We are able to find a factor since it follows that we can write

$$24779170^2 - 1 \equiv 0 \mod n$$

and therefore

$$(24779170 + 1)(24779170 - 1) \equiv 0 \mod n.$$

Trying to compute the gcd of 24779170 + 1 and n, we have

$$\begin{aligned}
31864033 &= (1)24779171 + 7084862 \\
24779171 &= (3)7084862 + 3524585 \\
7084862 &= (2)3524585 + 35692 \\
3524585 &= (98)35692 + 26769 \\
35692 &= (1)26769 + 8923 \\
26769 &= (3)8923
\end{aligned}$$

Therefore we have that 8923 is a factor of n. In particular, we can write $n = (8923)(3571)$.

2. Show that if p is a prime, then the congruence $x^2 \equiv a^2 \mod p$ has exactly two solutions.

Solution. We assume here that we want to find x in $\mathbb{Z}_p$, otherwise there can be more than two solutions (for example, 1, 4, and 6 are congruent to $1 = 1^2 \mod 5$). We can write

$$x^2 - a^2 \equiv 0 \mod p$$

and thus

$$(x + a)(x - a) \equiv 0 \mod p.$$

We can see that $x = a$ is one obvious solution since

$$(a - a) \equiv 0 \mod p.$$

To find the other, we recognize that $p \equiv 0 \mod p$ and therefore using $x = p - a$ we have

$$(p - a + a) \equiv p \equiv 0 \mod p.$$

To show these are the only two solutions, suppose there exists some new additional x' that solves the congruence. Then

$$(x' + a)(x' - a) \equiv 0 \mod p$$

so $x' = a$ or $x' = -a$. The former solution has already been shown. The latter implies $x' = p - a$ since $-a \equiv p - a \mod p$. So the two shown are the only solutions.

3. Solve for x and y

$$\begin{aligned}
2x + 3y &\equiv 8 \mod 17 \\
7x - y &\equiv 7 \mod 17
\end{aligned}$$

explaining, as you go, why this works.

Solution. Start by considering the second equation. We have

$$\begin{aligned} 7x - y &\equiv 7 \mod 17 \\ 7x - 7 &\equiv y \mod 17 \\ 7(x-1) &\equiv y \mod 17 \\ x - 1 &\equiv (7)^{-1}y \mod 17 \\ x - 1 &\equiv 5y \mod 17 \\ x &\equiv 5y - 1 \mod 17 \end{aligned}$$

and we know that $7^{-1} \mod 17$ is 5 since $(5)(7) = 35 \equiv 1 \mod 17$. Then we can substitute into the first equation to obtain

$$\begin{aligned} 10y - 2 + 3y &\equiv 8 \mod 17 \\ 13y &\equiv 6 \mod 17 \\ y &\equiv (13)^{-1}(6) \mod 17 \\ y &\equiv (4)(6) \mod 17 \\ y &\equiv 7 \mod 17 \end{aligned}$$

where we know the inverse of 13 mod 17 is 4, as $(4)(13) = 52 \equiv 1 \mod 17$. So we find x to be

$$x \equiv 5(7) + 1 \equiv 2 \mod 17.$$

We can verify in the original equations, giving

$$2(2) + 3(7) = 25 \equiv 8 \mod 17$$

and

$$7(2) - (7) = 7 \equiv 7 \mod 17.$$

This process of solution works because addition and multiplication are the same as with ordinary integers, with the exception of finding inverses. So we can solve the system as we would any Diophantine system, as long as we are careful to compute inverses mod 17.

4. Find all solutions to

$$x^2 \equiv 13 \mod 391$$

explaining, as you go, why this works.

Solution. We factor 391 to obtain a prime factorization of $17 \cdot 23$. Then we would like to solve

$$x^2 \equiv 13 \mod 17$$

and

$$x^2 \equiv 13 \mod 23.$$

In the former congruence, we compute solutions by brute force, giving $x = 8$ and $x = 9$. In the latter, we obtain $x = 6$, $x = 17$. Consider the solution pair (8, 6). We want

$$x \equiv 8 \mod 17$$

and

$$x \equiv 6 \mod 23.$$

We therefore apply the Chinese Remainder Theorem to solve

$$17x \equiv 1 \mod 23$$

and

$$23x \equiv 1 \mod 17$$

and obtain

$$x = 17 \cdot 19 \cdot 6 + 23 \cdot 3 \cdot 8 = 2490 \equiv 144 \mod 391.$$

Similarly for the pair (6, 9) we consider

$$x = 17 \cdot 19 \cdot 6 + 23 \cdot 3 \cdot 9 = 2559 \equiv 213 \mod 391.$$

Recalling the symmetry in finding square roots regarding positive and negative solutions, we try finding -144 and -213 mod 391; they are 247 and 178, respectively. Next, we verify the solutions:

$$\begin{aligned} 144^2 &= 20736 \equiv 13 \mod 391 \\ 213^2 &= 45369 \equiv 13 \mod 391 \\ 247^2 &= 45369 \equiv 13 \mod 391 \\ 178^2 &= 31684 \equiv 13 \mod 391. \end{aligned}$$

5. Use the facts that $n = 12509443$ is known to be the product of two primes and $\phi(n) = 12501720$ to find the two prime factors. Explain carefully why this works.

Solution. Let the prime factors be denoted by p and q. We know that

$$\phi(n) = (p-1)(q-1) = pq - (p+q) + 1$$

since p and q are necessarily relatively prime. Therefore, we have a system of equations

$$\begin{aligned} p + q &= n + 1 - \phi(n) \\ pq &= n. \end{aligned}$$

Computing the first, we obtain $p + q = 7724$. Next we make the substitution $p = 7724 - q$ and obtain

$$n = q(7724 - q) = 7724q - q^2$$

giving a quadratic $q^2 - 7724q + n$. Finding the roots with the quadratic formula, we obtain $q = 2311$ and $q = 5413$. We confirm that $2311 + 5413 = 7724$ and $2311(5413) = 12509443 = n$.

6. Use Miller's test (and your software) to prove that 661563014968918056308911823657 is a composite number.

Solution. Call the number above n for brevity's sake. As we are allowed to use our software, I begin by running my implementation of Miller-Rabin from homework 2 to confirm that n is indeed composite. In particular, we have a witness of $x = 141618362225198057430240896320$. Fermat's little theorem states that if $p \nmid a$,

$$a^{p-1} \equiv 1 \mod p.$$

In our case, n does not divide x as $n > x$, and we can compute

$$a^{p-1} \equiv 172393582718724122028152829190 \not\equiv 1 \mod p$$

so from the contrapositive of Fermat's little theorem, n is composite.