Ma 6a PS2

Om Sanan

October 2025

§1 Find all $x \in \mathbb{Z}$ such that $35x \equiv 10 \pmod{50}$.

Compute the greatest common divisor:

$$\gcd(35, 50) = 5.$$

Divide the entire equation by 5:

$$7x \equiv 2 \pmod{10}.$$

Find the multiplicative inverse of 7 mod 10:

$$7 \cdot 3 = 21 \equiv 1 \pmod{10}.$$

The inverse of 7 is 3.

Multiply both sides by 3:

$$x \equiv 3 \cdot 2 \equiv 6 \pmod{10}.$$

The reduced solution is

$$x \equiv 6 \pmod{10}.$$

Because we divided the original modulus 50 by $\gcd(35, 50) = 5$, we must lift the solutions back to mod 50:

$$x \equiv 6 + 10k \pmod{50}, \quad k = 0, 1, 2, 3, 4.$$

$$\boxed{x = 6,\ 16,\ 26,\ 36,\ 46 \pmod{50}.}$$

§2 Find all integers that leave remainders 1, 2, and 3 when divided by 9, 8, and 7, respectively

We are asked to find all integers x such that

$$x \equiv 1 \pmod{9}, \quad x \equiv 2 \pmod{8}, \quad x \equiv 3 \pmod{7}.$$

Since 9, 8, and 7 are pairwise coprime, there exists a unique solution modulo

$$N = 9 \cdot 8 \cdot 7 = 504.$$

Using CRT, let

$$N_1 = \frac{N}{9} = 56, \quad N_2 = \frac{N}{8} = 63, \quad N_3 = \frac{N}{7} = 72.$$

Next, find the inverses of N_i modulo their respective moduli:

$$\begin{aligned} 56 \equiv 2 \pmod{9} &\implies 2^{-1} \equiv 5 \pmod{9}, \\ 63 \equiv 7 \pmod{8} &\implies 7^{-1} \equiv 7 \pmod{8}, \\ 72 \equiv 2 \pmod{7} &\implies 2^{-1} \equiv 4 \pmod{7}. \end{aligned}$$

Then, the combined congruence is given by

$$x \equiv 1 \cdot 56 \cdot 5 + 2 \cdot 63 \cdot 7 + 3 \cdot 72 \cdot 4 \pmod{504}.$$

Simplifying,

$$x \equiv 280 + 882 + 864 = 2026 \equiv 10 \pmod{504}.$$

$$\boxed{x = 10 + 504k, \quad k \in \mathbb{Z}.}$$

§3 Prove that if an odd integer $n > 1$ is not a prime or a prime power, then there exists a nontrivial square root of 1 modulo n

Since n is odd and not a prime power, it has at least two odd prime factors. Therefore

$$n = \prod_{i=1}^{t} p_i^{e_i} \qquad (t \geq 2,\ p_i \text{ odd primes},\ e_i \geq 1).$$

Now, let's pick two distinct indices, say 1 and 2. By CRT, there exists an integer x satisfying the simultaneous congruences

$$x \equiv 1 \pmod{p_1^{e_1}}, \qquad x \equiv -1 \pmod{p_2^{e_2}}, \qquad x \equiv 1 \pmod{p_i^{e_i}} \text{ for } i = 3, \ldots, t.$$

For each i, we then have $x^2 \equiv 1 \pmod{p_i^{e_i}}$, hence by CRT again,

$$x^2 \equiv 1 \pmod{n}.$$

Moreover, $x \not\equiv 1 \pmod{n}$ because $x \equiv -1 \pmod{p_2^{e_2}}$, and $x \not\equiv -1 \pmod{n}$ because $x \equiv 1 \pmod{p_1^{e_1}}$.

$$\boxed{\text{Therefore, } x \text{ is a nontrivial square root of 1 modulo } n.}$$

§4 Decrypt an RSA message (01↔A, . . . , 26↔Z) with $e = 5$, $n = 2881$: 2688 0559 0752 0915 2112 0564 2743 2783

Setup (per RSA method in class). Factor n: $2881 = 43 \cdot 67$ (both prime), so

$$\varphi(n) = (43 - 1)(67 - 1) = 42 \cdot 66 = 2772.$$

Compute the decryption exponent $d \equiv e^{-1} \pmod{\varphi(n)}$ for $e = 5$:

$$5d \equiv 1 \pmod{2772} \quad \Rightarrow \quad d = 1109.$$

Decryption proces. For each ciphertext block C, compute $M \equiv C^d \pmod{n}$ and then split M into two 2-digit numbers (01–26) to map back to letters.

C	$M \equiv C^{1109} \pmod{2881}$	2-digit split	Letters
2688	715	07 | 15	$G\,O$
0559	301	03 | 01	$C\,A$
0752	1220	12 | 20	$L\,T$
0915	503	05 | 03	$E\,C$
2112	802	08 | 02	$H\,B$
0564	501	05 | 01	$E\,A$
2743	2205	22 | 05	$V\,E$
2783	1819	18 | 19	$R\,S$

Result:

$$\boxed{\text{GO CALTECH BEAVERS}}$$

§5 The number 1288119601 is composite. Find a Miller–Rabin witness.

We are given $n = 1288119601$. Then

$$n - 1 = 1288119600 = 2^4 \cdot 80507475, \quad \therefore \quad (s = 4,\ d = 80507475).$$

Take base $a = 2$. Compute

$$x_0 \equiv 2^d \pmod{n} \equiv 95{,}382{,}061 \not\equiv 1 \pmod{n}.$$

Then let's continuously square modulo n:

$$x_1 \equiv x_0^2 \equiv 2{,}066{,}916, \quad x_2 \equiv x_1^2 \equiv 737{,}154{,}140, \quad x_3 \equiv x_2^2 \equiv 745{,}370{,}093 \pmod{n}.$$

None of x_0, x_1, x_2, x_3 is congruent to $-1 \pmod{n}$ (i.e. to $n - 1 = 1{,}288{,}119{,}600$). Since $x_0 \not\equiv 1 \pmod{n}$ and no other one hits $-1 \pmod{n}$, the base

$$\boxed{a = 2}$$

is a Miller-Rabin witness. (I think $a = 3, 5, \ldots$ also works.)