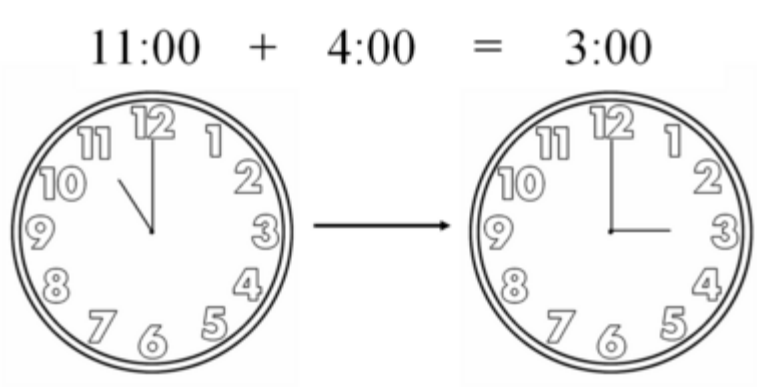

Congruences: aka Clock Arithmetic

Fermat, then Euler, **Joseph-Louis Lagrange** (Italian mathematician and astronomer; 1736 1813), and **Adrien-Marie Legendre** (French mathematician; 1752 - 1833), found clever indirect methods to work with gigantic numbers of the sort considered above. This enabled them to make the most significant advances in number theory during the sixteen and seventeenth centuries. But it was the brilliant Gauss who unified their methods and results. His masterpiece, *Disquisitiones Arithmeticae*, was written at the age of twenty and yet it "not only began the modern theory of numbers but determined the directions of work in the subject up to the present time."[1]

In this work Gauss introduces the *theory of congruences* which you might already know as *clock* or *modular arithmetic*. Simply enough, 7 hours after 11 o'clock will be 6 o'clock. We write this as

$$7 + 11 \equiv 6 \pmod{12}$$

which we read as "7 plus 11 is congruent to 6 mod 12." The military uses 24-hour clocks so we would have

$$7 + 11 \equiv 18 \pmod{24}.$$

However, 7 hours after 23 hundred hours (i.e., 11 o'clock p.m.) is 6 hundred hours:

$$7 + 23 \equiv 6 \pmod{24}.$$

Gauss noticed that we can define congruences like this for any "clock." We say that $7+23 \equiv 6 \pmod{24}$ because $7+23 = 30$ and the remainder when 30 is divided by 24 is 6. So we will say a is **congruent** to r mod m and write $a \equiv r \pmod{m}$ whenever a leaves remainder r when divided by m. The remainder r is called the **residue** and the base m of the "clock" is called the **modulus**. In his *Disquisitiones*, Gauss showed that congruences form arithmetical systems where we can not only add numbers, but subtract, multiply and exponentiate numbers, as well.

---

[1] Morris Kline, from *Mathematical Thought from Ancient to Modern Times*, Oxford University Press, 1972, p 813

There is a slight inconsistency with the mathematical definition and the description using clocks. Namely, using a clock we would say $5 + 7 \equiv 12 \pmod{12}$ since 5 hours after 7 o'clock is 12 o'clock. Indeed, the numbers on a standard clock are 1 − 12. But, when we consider this congruence with remainders we have $5+7 \equiv 0 \pmod{12}$ since the remainder when 5+7 is divided by 12 is 0. For mathematicians mod 12 arithmetic uses the numbers 0− 11 instead of 1 − 12 with 0 taking the place of 12. While the mathematicians approach is best for a deep study of modular arithmetic, for our purposes here either convention will be appropriate.

Application of Congruences

In one of his remarkable insights, Euler "noticed" that the Mersenne number $M_{83} = 2^{83} - 1 =$ 9,671,406,556,917,033,397,649,408 was not prime but rather had 167 as a factor. "Noticing" this is remarkable, it seems to be an unpleasant task to check that 167 divides this gigantic number. Let's see how we can use congruences to do this.

If 167 is a factor of $2^{83} - 1$, then this means 167 divides $2^{83} - 1$ evenly. Another way to say this is there is no remainder, which means $2^{83} - 1 \equiv 0 \pmod{167}$ So how can we compute powers of 2 mod 167? Well,

$$2^8 = 256 \text{ so } 2^8 \equiv 256 \pmod{167} \equiv 89 \pmod{167}.$$

Since $(2^8)^2 = 2^{16}$, we have

$$2^{16} \equiv (89 \pmod{167})^2 \equiv 89^2 \pmod{167} \equiv 7921 \pmod{167} \equiv 72 \pmod{167}.$$

Similarly,

$$2^{32} \equiv 72^2 \pmod{167} \equiv 5184 \pmod{167} \equiv 7 \pmod{167}, \text{ and}$$
$$2^{64} \equiv 7^2 \pmod{167} \equiv 49 \pmod{167}.$$

So then

$$2^{83} \equiv \left(2^{64} \pmod{167}\right) \times \left(2^{16} \pmod{167}\right) \times \left(2^3 \pmod{167}\right)$$
$$\equiv (49 \times 72 \times 8) \pmod{167} \equiv 28224 \pmod{167} \equiv 1 \pmod{167}.$$

Hence, $2^{83} - 1 \equiv (1 - 1) \pmod{167} \equiv 0 \pmod{167}$.

This is a very powerful method indeed. In fact, without methods like these, the computations that are necessary to encrypt messages, with algorithms like the RSA would not be feasible.

Powers and Congruences

1. Reduce each of the congruences below to a number smaller than the modulus, 3:

$1^2 \equiv$ _____ (mod 3)
$2^2 \equiv$ _____ (mod 3)
$3^2 \equiv$ _____ (mod 3)
$4^2 \equiv$ _____ (mod 3)
$5^2 \equiv$ _____ (mod 3)
$6^2 \equiv$ _____ (mod 3)
$7^2 \equiv$ _____ (mod 3)

2. Do you see a pattern in your answers to Investigation **1**? If so, do you think it will continue indefinitely? Explain why.

3. Reduce each of the congruences below to a number smaller than the modulus, 4:

$1^3 \equiv$ _____ (mod 4)
$2^3 \equiv$ _____ (mod 4)
$3^3 \equiv$ _____ (mod 4)
$4^3 \equiv$ _____ (mod 4)
$5^3 \equiv$ _____ (mod 4)
$6^3 \equiv$ _____ (mod 4)
$7^3 \equiv$ _____ (mod 4)

4. Do you see a pattern in your answers to Investigation **3**? If so, do you think it will continue indefinitely? Explain why.

5/ Reduce each of the congruences below to a number smaller than the modulus, 5:

$1^4 \equiv$ _____ (mod 5)
$2^4 \equiv$ _____ (mod 5)
$3^4 \equiv$ _____ (mod 5)
$4^4 \equiv$ _____ (mod 5)
$5^4 \equiv$ _____ (mod 5)
$6^4 \equiv$ _____ (mod 5)
$7^4 \equiv$ _____ (mod 5)

6. Do you see a pattern in your answers to Investigation **5**? If so, do you think it will continue indefinitely? Explain why.

7. Reduce each of the congruences below to a number smaller than the modulus, 6:

$1^5 \equiv$ _____ (mod 6)
$2^5 \equiv$ _____ (mod 6)
$3^5 \equiv$ _____ (mod 6)
$4^5 \equiv$ _____ (mod 6)
$5^5 \equiv$ _____ (mod 6)
$6^5 \equiv$ _____ (mod 6)
$7^5 \equiv$ _____ (mod 6)

8. Do you see a pattern in your answers to Investigation **7**? If so, do you think it will continue indefinitely? Explain why.

9. Reduce each of the congruences below to a number smaller than the modulus, 7:

$1^6 \equiv$ _____ (mod 7)
$2^6 \equiv$ _____ (mod 7)
$3^6 \equiv$ _____ (mod 7)
$4^6 \equiv$ _____ (mod 7)
$5^6 \equiv$ _____ (mod 7)
$6^6 \equiv$ _____ (mod 7)
$7^6 \equiv$ _____ (mod 7)

10. Do you see a pattern in your answers to Investigation **63**? If so, do you think it will continue indefinitely? Explain why.

11. You should see some patterns emerging that tie together some of the of the groups of congruence computations. Make one or more conjectures describing congruences of the form

$$a^{n-1} \bmod n,$$

based on properties of the numbers a and n.