Modular Arithmetic and Division

Quotient- Remainder Theorem:
Given positive integers a and d, there exist integers q and r such that,

$$a = dq + r, \qquad r < d$$

Divisor, quotient, remainder

$q = a \text{ div } d$
$r = a \bmod d$

Example: $30 \text{ div } 7 = 4$
$30 \bmod 7 = 2$

Greatest Common Divisor:
The GCD for integers a and b the largest integer that divides both a and b. To efficiently find the greatest common divisor you can use the Euclidean Algorithm.

Two lemmas are needed:

1. gcd(r,0) = r
2. If a=dq+r, then gcd(a,d)=gcd(d,r)

Example: Find gcd (408,120)

gcd(408,120)
= gcd(120,48)
= gcd(48,24)
= gcd(24,0)
= 24

$408 = \mathbf{3} \times 120 + \mathbf{48}$
$120 = 2 \times 48 + \mathbf{24}$
$48 = 2 \times 24 + 0$

sample rough work

$$\begin{array}{r} 3 \\ 120 \overline{)\ 408} \\ -\ 360 \\ \hline 48 \end{array}$$

Practice: Practice: Find gcd(5280,1360) using the Euclidean Algorithm. Answer: 80

The algorithm helps to reduce larger computations into smaller ones and this is also a benefit of modular arithmetic.

Congruence: $a \equiv b \pmod n$, a and b are congruent modulo n if they have the same reminders when divided by n

Examples: $30 \equiv 2 \pmod 7$, $9 \equiv 1 \pmod 2$, $21 \equiv 5 \pmod 8$, etc.

Modular Equivalences:

For the integers a, q, r, and d > 0, the following statements are equivalent:

1. $a = dq+r$
2. $a \equiv r \pmod d$
3. $a \pmod d = r \pmod d$
4. $n \mid (a - r)$
5. a and r have the same (nonnegative) remainder when divided by d

Modular Arithmetic:

Let a, b, c, d, and n be integers with $n > 1$ where $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then

1. $ab \equiv [(a \bmod n)(b \bmod n)] \bmod n$
2. $(a+b) \equiv (c+d) \pmod{n}$
3. $a^k \equiv c^k \pmod{n}$ for all integers k
4. $a^k \pmod{n} = (a \bmod n)^k \bmod n$
5. If p is prime and a is not divisible by p, $a^{(p-1)} \equiv 1 \pmod{p}$ [Fermat's Little Theorem]

Use modular arithmetic in the following examples to convert large number computations into smaller number computations. It can be beneficial to do this in cryptography for example, when the numbers can be over a thousand digits long, taking up more memory and time.

Tip: When using a calculator to compute the remainder, use the formula:

$a \bmod n = a - d \cdot \left\lfloor \frac{a}{n} \right\rfloor$

Example: $103 \bmod 12 = 103 - 12\left\lfloor \frac{103}{12} \right\rfloor = 103 - 12(8) = 7$

Some examples using modular arithmetic:

1. $(3-20) \bmod 5 = 3 \bmod 5 - 20 \bmod 5 = 3 - 0 = 3$ or since $-17 = -4 \cdot (5) + 3$
2. $-8 \equiv 2 \bmod 5$ since $-8 = -2 \cdot (5) + 2$
3. $(12+8) \bmod 5 = 0$ or we can say $(12 + 8) \bmod 5 \equiv 0 \bmod 5$
4. Since $26 \bmod 4 = 2$, $26^2 5 \bmod 4 \equiv 2^2 5 \bmod 4 = 20 \bmod 4 = 0$

Using Fermat's Little Theorem:

5. $4^{17} \pmod{11}$
   $= 4^{(10+7)} \pmod{11}$
   $= 4^{10} 4^7 \pmod{11}$ $\quad 4^{10} \equiv 1 \pmod{11} = 1$ **since 11 is prime**
   $\equiv 4^{2+2+2+1} \pmod{11}$
   $\equiv 4^2 4^2 4^2 4^1 \pmod{11}$
   $\equiv 5 \cdot 5 \cdot 5 \cdot 4 \pmod{11}$
   $= 125 \cdot 4 \pmod{11}$
   $\equiv 4 \cdot 4 \pmod{11}$
   $\equiv 5 \pmod{11}$

So, $4^{17} \pmod{11} = 5$

6. **Practice:** Show that $3^{26} \bmod 5 = 4$

Student Learning Centre

Call: 905.721.8668 ext. 6578
Email: studentlearning@ontariotechu.ca
Website: ontariotechu.ca/studentlearning
Downtown Oshawa Location: Charles Hall
North Oshawa Location: Shawenjigewining Hall

OntarioTech UNIVERSITY