# Modular Arithmetic

Reduction modulo a polynomial $g(x)$ or modulo an integer $m$ plays a central role in the mathematics of cryptography. Recall that for a monic polynomial $g(x)$ of positive degree, we define $a(x) \bmod g(x)$ to the unique polynomial $a_0(x)$ with $\deg a_0(x) < \deg g(x)$ such that

$$a(x) = a_0(x) + a_1(x)g(x).$$

For an integer $m$, we define $a \bmod m$ to be the unique integer $a_0$ with $0 \leq a_0 < m$ such that $a = a_0 + a_1 m$.

**Fermat's little theorem**. If $p$ is a prime, then the relation $a^{p-1} \equiv 1 \bmod p$ holds for any integer $a$ not divisible by $p$.

Note. The Magma function mod is the binary operator, with the syntax:

```
> m := 101;
> 2^31 mod m;
34
```

The same result can be achieved with the Modexp, or modular exponentiation function:

```
> Modexp(2,31,m);
34
```

2. Let $p$ be the prime $2^{31} - 1 = 2147483647$. Use the Magma function Modexp to verify Fermat's little theorem for several values of $a$. *Why would it be a bad idea to compute $a^{p-1}$ and then reduce modulo $p$?*

**Chinese remainder theorem**. Let $p$ and $q$ be distinct primes, then for every integer $a$ and $b$ there exists a unique integer $c$ with $0 \leq c < pq$ such that $c \equiv a \bmod p$ and $c \equiv b \bmod q$.

If $a$, $b$, and $c$ are as above, then for any integral polynomial $f(x)$, the integer $f(c)$ satisfies $f(c) \equiv f(a) \bmod p$ and $f(c) \equiv f(b) \bmod q$. Therefore $f(c) \bmod pq$ is the unique solution to the Chinese remainder theorem.

3. Let $p$ be as above and let $q = (2^{61} + 1)/3 = 768614336404564651$. Compute $a^{p-1} \bmod pq$ for various primes using Modexp. Then reduce the result modulo $p$. How do you explain the result in terms of the Chinese remainder theorem and Fermat's little theorem?

Analogues of Fermat's little theorem also hold for polynomials.

**Polynomial analogue of Fermat**. If $g(x)$ is an irreducible polynomial of degree $n$ over $\mathbb{F}_2$, then the relation $a(x)^{2^n-1} \equiv 1 \bmod g(x)$ holds for any polynomial $a(x)$ not divisible by $g(x)$.

**Chinese remainder theorem**. Let $g(x)$ and $h(x)$ be monic polynomials with no common factors. Given any polynomials $a(x)$ and $b(x)$, there exists a unique polynomial $c(x)$ such that $c(x) \equiv a(x) \bmod g(x)$ and $c(x) \equiv b(x) \bmod h(x)$.

We can create and work with polynomials over $\mathbb{F}_2$ as demonstrated by the following `Magma` code.

```
> F2 := FiniteField(2);
> P2<x> := PolynomialRing(F2);
> f := x^17 + x^5 + 1;
> Factorization(f);
[
<x^17 + x^5 + 1, 1>
]
```

4. Let $g(x) = x^{17} + x^5 + 1$, and use the function `Modexp` to verify the polynomial analogue of Fermat's little theorem for the polynomials $x$, $x^2 + x + 1$, etc.

5. Let $h(x) = x^{17} + x^{15} + x^{10} + x^5 + 1$ and compute $a(x)^{2^{17}-1} \bmod g(x)h(x)$ for various $a(x)$. What is the result reduced modulo $g(x)$? Why does the same not hold true for $a(x)^{2^{17}-1} \bmod g(x)h(x)$, reduced modulo $h(x)$?