The University of Sydney
Math3024 Elementary Cryptography and Protocols

Semester 1 **Exercises and Solutions for Week 10** 2004

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 mathematical result can be achieved with the `Modexp`, or modular exponentiation function:

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

The latter construction, however, in general is more efficient.

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.

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>
]
```

1. 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?*

   Solution The function `Modexp(a,e,p)` computes the result of $a^e \bmod p$ by doing an optimal number of squarings and multiplications, and reducing the intermediate results. The size of the expanded result a^e for large e, such as for $e = p-1 = 2^{31}-2$, would overflow the internal storage capacity of a computer, so it would be unwise to attempt to structure the algorithm as $a \mapsto a^e$ then to reduce modulo p.

2. 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?

   Solution For primes $p = 2^{31}-1$ and $q = (2^{61}-1)/3$, we compute for $a = 2$ the power $\texttt{Modexp}(2, p-1, pq) = 1031616713335618410196063 58$. If we reduce modulo q, then result is $624491483287 08779$ — pretty much a random number of size q. On the other hand, if we reduce modulo p, the result is 1. This follows from Fermat's little theorem, since $\texttt{Modexp}(2, p-1, pq) \bmod p$ is equal to the result $\texttt{Modexp}(2, p-1, p)$.

3. 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.

   Solution For the polynomial $g(x) = x^{17}+x^5+1$, we should use exponent $e = 2^{17}-1$, which we note is prime. We verify that each of the results $\texttt{Modexp}(x, e, g)$ and $\texttt{Modexp}(x^2 + x + 1, e, g)$ is 1. Since e is prime, this proves that $g(x)$ is not only irreducible, but also primitive.

4. 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 $h(x)$?

Solution With $g(x)$ as above and $h(x) = x^{17} + x^{15} + x^{10} + x^5 + 1$, the results $\texttt{Modexp}(x, e, gh) \bmod g = 1$ holds as expected, exactly as in the third question. In this case, if $h(x)$ is also irreducible, then the result:

$$\texttt{Modexp}(x, e, gh) \bmod h = x^{16} + x^{15} + x^{14} + x^{11} + x^{10} + x^8 + x^6 + x^3 + 1$$

would also have been 1. The fact that this result does not give 1 is a consequence of the reducibility of h:

$$h = (x^3 + x^2 + 1)(x^{14} + x^{13} + x^{11} + x^8 + x^5 + x^4 + x^3 + x^2 + 1).$$