8

Homework 6 Cryptography

Rick Staals 0716184
Erwin van Duijnhoven 0719562

October 16, 2013

1 Exercise 1

Consider the residue classes of $\mathbb{F}_2[x]$ modulo $f(x) = x^n + 1$ for some positive integer $n > 1$, i.e. $R = \mathbb{F}_2[x]/(x^n + 1)$. Note that R can be represented as

$$R = \{a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1}x^{n-1} | a_i \in \mathbb{F}_2\}$$

Show that R is not a field, i.e. find a non-zero element that is not invertible or that gives 0 when multiplied with another non-zero element.

1.1 Answer

2/2

nonzero

If we take the elements $x+1$ and $1+x+x^2+\ldots+x^{n-1}$ then the two multiplied is equal to $x^n + 1$. This is equal to zero, therefore R is not a field.

$x^n + 2x^{n-1} + \cdots + 2x^2 + 2x + 1$

2 Exercise 2

Let K be a field of characteristic p, where p is prime. Show that for any integer $n \geq 0$ one has

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$

for all $a, b \in K$.
Hint: You can use the binomial theorem and use proof by induction.

2.1 Answer

3/4

By the binomial theorem we know.

$$(a+b)^p = a^p + pa^{p-1}b + (p(p-1)/2!)a^{p-2}b^2 + \ldots + b^p$$

for prime p

Because every binomial coefficient except the first and last is divisible by p, this reduces to

explain...

$$(a+b)^p = a^p + b^p$$

OK, proven for $n=1$. And $n=0$?

By induction we now only have to prove that the same is true for $n+1$, where we assume it is true for $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.

$$
\begin{aligned}
&(a+b)^{p^{n+1}} \\
&= ((a+b)^{p^n})^p \\
&= (a^{p^n} + b^{p^n})^p \\
&= (a^{p^n})^p + p(a^{p^n})^{p-1}(b^{p^n}) + (p(p-1)/2!)(a^{p^n})^{p-2}(b^{p^n})^2 + \ldots + (b^{p^n})^p \\
&= a^{p^{n+1}} + a^{p^{n+1}}
\end{aligned}
$$

It is true for $n+1$ so by induction it is true for all $n \geq 0$.

1

3 Exercise 3

Compute $N_3(4)$, the number of irreducible polynomials of degree 4 over $\mathbb{F}_3$.

2/2

3.1 Answer

By the lemma given in class we know the following

$$N_q(m) = \frac{1}{m}(q^M - \sum_{d|m, d\neq m} dN_q(d))$$

We also know that $N_q(1) = q$. In this particular case it means that.

$$
\begin{aligned}
N_3(2) &= \tfrac{1}{2}(3^2 - 1 \cdot N_3(1)) = 3 \\
N_3(4) &= \tfrac{1}{4}(3^4 - 2 \cdot N_3(2) - 1 \cdot N_3(1)) \\
&= \tfrac{1}{4}(3^4 - 2 \times 3 - 3) = 18
\end{aligned}
$$

therefore the number of irreducible polynomials of degree 4 over $\mathbb{F}_3$ is 18.

4 Exercise 4

Use the Rabin test to prove that $x^{121} + x^2 + 1$ is not irreducible over $\mathbb{F}_2$. For this exercise you should use a computer algebra system. Please document the results of all steps in the algorithm and show how they were obtained; show how you worked around needing to work with polynomials of degree 2^{121}.

1/2

4.1 Answer

We use the Rabin test on $f = x^{121} + x^2 + 1$.
This means that $n = 121$ and $n_1 = \frac{n}{p_1} = \frac{121}{11} = 11$.
Because we only have one prime divisor of 121, the algorithm only has one step.
$h = x^{(2^{11})} + x \mod f = x^{112} + x^{25} + x^{23} + x$.
If $gcd(h, f) = 1$, f possibly is irreducible over $\mathbb{F}_2$.
To calculate this, we use Mathematica. We get $PolynomialGCD[x^{112} + x^{25} + x^{23} + x, x^{121} + x^2 + 1, Modulus -> 2]$, so f possibly is irreducible over $\mathbb{F}_2$. $=?$
The only thing we need to check now is if f is a divisor of $x^{2^{121}} + x$, therefor we calculate $PolynomialMod[x^{(2^{121})} + x, x^{121} + x^2 + 1, Modulus -> 2]$. The answer is a very large polynomial of degree 120, but not 0. Therefore f is not irreducible over $\mathbb{F}_2$.

how do you handle $x^{2^{121}}$ in Mathematica?