CS60094: Computational Number Theory, Spring 2018-19
Class Test 3

CSE 107, 12 PM — 18th April, 2019

Duration = 55 minutes — Total marks = 20

1. Prove that $f(x) \in \mathbb{F}_q[x]$ of degree two is irreducible if and only if $f(x)$ has no roots in $\mathbb{F}_q$. **[6]**

   Solution: Suppose that $f(x)$ is irreducible. If $f(\alpha) = 0$ for some $\alpha \in \mathbb{F}_q$, then $(x - \alpha) \mid f(x)$ causing $f(x)$ to split into two linear factors over $\mathbb{F}_q$. This contradicts that $f(x)$ is irreducible over $\mathbb{F}_q$. So $f(x)$ has no roots in F_q.

   Conversely, suppose that $f(x)$ has no roots in $\mathbb{F}_q$. Given that $\deg f(x) = 2$, the only possible factors are linear or constant factors. Since $f(x)$ has no roots in $\mathbb{F}_q$, it cannot have linear factors over $\mathbb{F}_q$ and is therefore irreducible. (A polynomial is irreducible if it has no non-constant factors of strictly smaller degree.)

2. Determine whether the following polynomials are irreducible or not.

   (a) $x^{23} - 9x^{12} + 15 \in \mathbb{Z}[x]$. **[2]**

   Solution: We can use Eisenstein's criterion. Firstly, $\operatorname{cont}(x^{23} - 9x^{12} + 15) = \gcd(1, -9, 15) = 1$. Now, observe that $3|15$, $3^2 \nmid 15$ and $3|9$. Therefore the given polynomial is irreducible in $\mathbb{Z}[x]$.

   (b) $x^4 + 2x + 2 \in \mathbb{F}_3[x]$. **[2]**

   Solution: We have

   $$\gcd(x^3 - x, x^4 + 2x + 2) = 1,$$

   $$\gcd(x^{3^2} - x, x^4 + 2x + 2) = 1,$$

   and hence $x^4 + 2x + 2$ has no factors of degree ≤ 2, which means it is irreducible.

3. Find the square-free factorisation of $x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x + 1 \in \mathbb{F}_2[x]$. **[4]**

   Solution: Let $f(x) = x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x + 1$. Then $f'(x) = x^8 + x^6 + x^4 + 1 \neq 0$ and $g(x) = \gcd(f(x), f'(x)) = f'(x)$ as $f(x) = (x+1)f'(x)$. So, $x+1$ is one of the factors. We next factorise $f'(x)$. We have $f''(x) = 0$ and $f'(x) = (h(x))^2$ where $h(x) = x^4 + x^3 + x^2 + 1$. We now factorise $h(x)$. $h'(x) = x^2+1$ and $\gcd(h(x), h'(x)) = x+1$. $h(x)/(x+1) = x^3+x+1$ is one of the factors of $h(x)$. Lastly $x+1$ is a square-free factor of $j(x)$. Summing up, we have $f(x) = (x+1)(x^3+x+1)(x^3+x+1)(x+1)(x+1)$ as the sqaure-free factorisation of $f(x)$.

4. Recall that $\operatorname{Discr}(f(x)) = (-1)^{d(d-1)/2} a_d^{-1} \operatorname{Res}(f(x), f'(x))$. Prove that

   (a) $\operatorname{Discr}(a_1 x + a_0) = 1$ **[2]**

   Solution: Let $f(x) = a_1 x + a_0$. We have $d = 1$ and $f'(x) = a_1$. The Sylvester matrix $\operatorname{Syl}(f(x), f'(x))$ is a 1×1 matrix with entry a_1. So $\operatorname{Res}(f(x), f'(x)) = \det \operatorname{Syl}(f(x), f'(x)) = a_1$ and hence $\operatorname{Discr}(f(x)) = (-1)^0 a_1^{-1} a_1 = 1$.

   (b) $\operatorname{Discr}(a_2 x^2 + a_1 x + a_0) = a_1^2 - 4a_0 a_2$ **[4]**

   Solution: Let $f(x) = a_2 x^2 + a_1 x + a_0$. Clearly $d = 2$ and $2a_2 x + a_1$. We have

   $$\operatorname{Res}(f(x), f'(x)) = \det \begin{bmatrix} a_2 & a_1 & a_0 \\ a_1 & a_0 & 0 \\ 0 & a_1 & a_0 \end{bmatrix} = 4a_0 a_2^2 - a_2 a_1^2,$$

   and therefore $\operatorname{Discr}(f(x)) = (-1)^{(2\cdot 1)/2} a_2^{-1} (4a_0 a_2^2 - a_2 a_1^2) = a_1^2 - 4a_0 a_2$.