Factorization over finite fields

`(Due Date: Sunday May 15th)`

1. Suppose p is a prime, $f \in \mathbb{F}_p[x]$ has degree 4, and
$$\gcd(x^p - x, f) = \gcd(x^{p^2} - x, f) = 1.$$
What can you say about the factorization of f in $\mathbb{F}_p[x]$?

2. Trace the distinct-degree factorization algorithm on computing the decomposition of the squarefree polynomial
$$x^{17} + 2x^{15} + 4x^{13} + x^{12} + 2x^{11} + 2x^{10} + 3x^9 + 4x^8 4x^4 + 3x^3 + 2x^2 + 4x \in \mathbb{F}_5[x].$$
Tell from the ouptut only how many irreducible factors of degree i the polynomial f has, for all i.

3. Let $q \in \mathbb{N}$ be a prime power.
   (a) Prove that if r is a prime number, then there are $(q^r - q)/r$ distinct monic irreducible polynomials of degree r in $\mathbb{F}_q[x]$.
   (b) Now suppose that r is a prime power. Find a simple formula for the number of monic irreducible polynomials of degree r over $\mathbb{F}_q$.

4. Let $p \in \mathbb{N}$ be a prime and $f \in \mathbb{Z}[x]$ monic of degree n. Prove that the congruence $f(a) \equiv 0 \bmod p$ has n solutions $a \in \mathbb{Z}_p$ if and only if $f \bmod p$ is a factor of $x^p - x$.

5. Let q be a prime power and $f \in \mathbb{F}_q[x]$ squarefree of degree n.
   (a) Prove that for $1 \le a \le b \le n$, the polynomial $\gcd\left(\prod_{a \le d < b} x^{q^d} - x, f\right)$ is the product of all monic irreducible factors of f whose degree divides some number in the interval $\{a, a+1, \ldots, b-1\}$.
   (b) Determine $\gcd\left(\prod_{a \le d < b} x^{q^b} - x^{q^{b-d}}, f\right)$.
   (c) Consider the following *blocking strategy* for distinct degree factorization. We partition the set $\{1, \ldots, n\}$ of possible degrees of irreducible factors of f into k intervals $I_1 = \{c_0 = 1, 2, \ldots, c_1 - 1\}$, $I_2 = \{c_1, c_1 + 1, \ldots, c_2 - 1\}, \ldots, I_k = \{c_{k-1}, c_{k-1} + 1, \ldots, c_k - 1 = n\}$, with integers $1 = c_0 < c_1 < \ldots < c_k = n + 1$. Describe an algorithm which, on input f, computes the polynomials $g_1, \ldots, g_k$ such that g_j is the product of all monic irreducible factors of f with degree in the interval I_j for $1 \le j \le k$.

6. We consider $\mathbb{F}_{41}$.

(a) Draw the "squaring graph" in $\mathbb{F}_{41}^{\times}$, the directed graph on vertices $1, \ldots, 40$ with the edge (i, j) present if and only if $i^2 \equiv j$, mod 41, for $1 \leq i, j \leq 40$. Arrange your drawing so that the structure of the graphs is easy to see.

(b) Draw the "cubing graph" $i^3 \equiv j \bmod 41$.

(c) Draw the "fifth power graph" $i^5 \equiv j$, mod 41.

(d) Can you see the qualitative differences in the three graphs above? Can you explain them?

(e) Let q be a prime larger than 1000000. What can you say about the "qth power graph" on $\mathbb{F}_{41}^{\times}$?

(f) How many elements of $\mathbb{F}_{41}^{\times}$ are squares? How many are nonsquares? Same question for cubes and fifth powers.

7. Let $\mathbb{F}_q$ be a finite field with q elements, and $k \in \mathbb{N}$.

(a) For $q = 13$ and $q = 17$, draw the graph of the cubing map $a \mapsto a^3$ on $\mathbb{F}_q$, with the elements of $\mathbb{F}_q$ as vertices and an edge $a \to b$ present if and only if $a^3 = b$.

(b) Show that $\operatorname{ord}(a^k) = \operatorname{ord}(a)/\gcd(k, \operatorname{ord}(a))$ for all $a \in \mathbb{F}_q^{\times}$.

(c) Show that the kth power group homomorphism $\sigma_k : \mathbb{F}_q^{\times} \to \mathbb{F}_q^{\times}$ is an automorphism if and only if $\gcd(k, q-1) = 1$.

(d) Conclude that $\operatorname{Ker}(\sigma_k) = \operatorname{Ker}(\sigma_\ell)$ and $\operatorname{Im}(\sigma_k) = \operatorname{Im}(\sigma_\ell)$, with $\ell = \gcd(k, q-1)$.

8. The squarefree polynomial

$$\begin{aligned} f &= x^{18} - 7x^{17} + 4x^{16} + 2x^{15} - x^{13} - 7x^{12} + 4x^{11} + 7x^{10} + 4x^9 - 3x^8 - 3x^7 \\ &\quad +7x^6 - 7x^5 + 7x^4 + 7x^3 - 3x^2 + 5x + 5 \in \mathbb{F}_{17}[x] \end{aligned}$$

splits into 3 irreducible factors of degree 6.

(a) How would you check the above statement without factoring f, by computing at most three gcd's?

(b) Trace the equal-degree factorization algorithm in order to comute these factors.

(c) Design an efficient probabilistic algorithm that, given a prime p and an $a \in \mathbb{Z}_p^{\times}$, computes the square roots of $a \bmod p$ provided they exist. Apply your algorithm to $p = 2591$ and $a = 1005$.

9. Assume that $q - 1 = 2^k u$, with $k \geq 2$ and $u \in \mathbb{N}$.

(a) Let $S \subset \mathbb{F}_q^{\times}$ be the subgroup of 2^kth roots of unity. What is the order of S, and how many primitive 2^kth roots of unity are there?

(b) Show that $a^u \in S$ for all $a \in \mathbb{F}_q^\times$, and that $b = a^u$ is a primitive 2^kth root of unity with probability $\frac{1}{2}$ is a is chosen uniformly at random.

(c) Prove that b is a primitive 2^kth root of unity if and ony if $b^{2^{k-1}} = -1$.

(d) Design a probabilistic algorithm for finding a primitive 2^kth root of unity, and show that it uses an expected number of $\mathcal{O}(\log q)$ operations in $\mathbb{F}_q$, or $\mathcal{O}(\log q \cdot M(\log q))$ word operations. Use your algorithm to find a primitive 2^{59}th root of unity for $q = 27 \cdot 2^{59} + 1$.

10. Show that recursively applying the equal-degree splitting algorithm to the smaller factor leads to an algorithm for finding *one* irreducible factor of the input polynomial with an expected running time of $\mathcal{O}((d \log q + \log n)M(n))$.

11. For $m \in \mathbb{N}$, we define the mth *trace polynomial* over $\mathbb{F}_2$ by

$$T_m = x^{2^{m-1}} + x^{2^{m-2}} + \ldots + x^4 + x^2 + x \in \mathbb{F}_2[x].$$

Let $q = 2^k$ for some $k \in \mathbb{Z}_{>0}$, $f \in \mathbb{F}_q[x]$ squarefree of degree n, with $r \geq 2$ irreducible factors $f_1, \ldots, f_r \in \mathbb{F}_q[x]$, $R = \mathbb{F}_q[x]/\langle f \rangle$, $R_i = \mathbb{F}_q[x]/\langle f_i \rangle$, and $\chi_i : R \to \mathbb{R}_i$ the projection.

(a) Prove that $x^{2^m} + x = T_m(T_m + 1)$, and conclude that $T_m(\alpha) \in \mathbb{F}_2$ for any $\alpha \in \mathbb{F}_{2^m}$, and that both $T_m(\alpha) = 0$ and $T_m(\alpha) = 1$ occur with probability $\frac{1}{2}$ when α is chosen uniformly at random.

(b) Suppose that all irreducible factors of f have the same degree d. Show that $\chi_i(T_{kd}(\alpha)) \in \mathbb{F}_2$ for all $\alpha \in R$, and conclude that for a uniformly random $\alpha \in R$, we have $T_{kd}(\alpha) \in \mathbb{F}_2$ with probability $2^{1-r} \leq \frac{1}{2}$.

(c) Modify the equal-degree splitting algorithm so as to work for $q = 2^k$, by computing $b = T_{kd}(a) \operatorname{rem} f$ in step 3. Prove that the modified algorithm fails with probability at most $\frac{1}{2}$, and that its running time is the same as that of the original algorithm.

12. Apply the complete polynomial factorization over finite fields algorithm to factor the polynomial $x^6 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$ into irreducible factors. Show all your steps.

13. Let F be a field and $f \in F[x]$ with $f(0) \neq 0$. Recall that $\operatorname{rev}(f) = f^* = x^{\deg(f)} f(1/x)$, the reversal or reciprocal polynomial of f. We say that f is *self-reciprocal* if $f = f^*$.

(a) Show that $(f \cdot g)^* = f^* \cdot g^*$.

(b) Prove that $f(\alpha^{-1}) = 0 \iff f^*(\alpha) = 0$, for all $\alpha \in F$. Conclude that the set of zeroes of f is closed under inversion if f is self-reciprocal.

(c) Show that every self-reciprocal polynomial f of odd degree satisfies $f(-1) = 0$.

(d) Let $f \in F[x]$ with $f(0) \neq 0$ be self-reciprocal and $g \in F[x]$ an irreducible factor of f. Show that g^* is also an irreducible factor of f.

(e) The squarefree polynomial $f = (x^{21}+1)/(x+1) \in \mathbb{F}_2[x]$ has -among others- the following irreducible factors: x^2+x+1, x^3+x+1. and $x^6+x^4+x^2+x+1$. What are the others?

14. Prove or disprove:

(a) The polynomial $x^{1000}+2 \in \mathbb{F}_5[x]$ is squarefree.

(b) Let F be a field and $f, g \in F[x]$. Then the squarefree part of fg is the product of the squarefree parts of f and of g.

15. (a) Test the following polynomials for multiple factors in $\mathbb{Q}[x]$:

i. $x^3 - 3x^2 + 4$

ii. $x^3 - 2x^2 - x + 2$

(b) Compute the squarefree decomposition of the following polynomials in $\mathbb{Q}[x]$ and in $\mathbb{F}_3[x]$:

i. $x^6 - x^5 - 4x^4 + 2x^3 + 5x^2 - x - 2$

ii. $x^6 - 3x^5 + 6x^3 - 3x^2 - 3x + 2$

iii. $x^5 - 2x^4 - 2x^3 + 4x^2 + x - 2$

iv. $x^6 - 2x^5 - 4x^4 + 6x^3 + 7x^2 - 4x - 4$

v. $x^6 - 6x^5 + 12x^4 - 6x^3 - 9x^2 + 12x - 4$

16. Let $f \in \mathbb{Z}[x]$ be of degree n, and max-norm $\|f\|_\infty = A$, $f = (ux+v)g$, with nonzero $u, v \in \mathbb{Z}$ and $g = \sum_{i=0}^{n-1} g_i x^i \in \mathbb{Z}[x]$.

(a) Prove that $|g_i| < \frac{(i+1)A}{|v|}$ for $0 \leq i < n-1$ if $|u| = |v|$, and conclude then that $\|g\|_\infty \leq nA$.

(b) Now assume that $\alpha = |u/v| < 1$. show that $|g_i| \leq A(1-\alpha^{i+1})/(1-\alpha)|v|$ for $0 \leq i < n-1$, and conclude that $\|g\|_\infty \leq A$. Prove that the latter also holds if $|u/v| > 1$.