MATH 895, Assignment 4, Summer 2017

Instructor: Michael Monagan

Please hand in the assignment by 8:30am Thursday June 22nd.
Late Penalty −20% off for up to 26 hours late. Zero after that.

Question 1: Minimal polynomials.

(a) Using linear algebra, find the minimal polynomial $m(z) \in \mathbb{Q}[x]$ for

$$\alpha = 1 + \sqrt{2} + \sqrt{3}.$$

(b) Using the extended Euclidean algorithm compute the inverse of α i.e. $[z]^{-1}$ in $\mathbb{Q}[z]/(m)$.

(c) Let α be an algebraic number and $m(z)$ be a non-zero monic polynomial in $\mathbb{Q}[z]$ of least degree such that $m(\alpha) = 0$.
Prove that $m(z)$ is (i) unique and (ii) irreducible over $\mathbb{Q}$.

Question 2: Computing with algebraic numbers.

Let ω be a primitive 5th root of unity in $\mathbb{C}$. Consider the following linear system

$$\{ \ (\omega + 4)x + \omega y = 1, \ \omega^3 x + \omega^4 y = -1 \ \}$$

(a) Input ω in Maple using the RootOf representation for algebraic numbers and solve the linear system using the `solve` command.

(b) Now solve the system modulo $p = 31, 41, 61, \ldots$ and as many primes p as you need s.t. $5|(p-1)$. After you've done this you will recover the solutions using Chinese remaindering and rational number reconstruction. Use Maple's `ichrem` and `irratrecon` commands.

For each prime factor $m(z) = z^4 + z^3 + z^2 + z^1 + 1 \bmod p$ and solve the linear system modulo p by evaluating at the roots of $m(z)$ in $\mathbb{Z}_p$. Then using Chinese remaindering (interpolation) recover the solutions mod $m(z)$.

To compute the roots of $m(z)$ in $\mathbb{Z}_p$ use the `Roots(m) mod p` command.

To solve $Ax = b$ over $\mathbb{Z}_p$ use the `Linsolve(A,b) mod p` command.

Question 3: Trager's algorithm.

Let ω be a primitive **4**'th root of unity. Using Trager's algorithm, factor $f(x) = x^4+x^2+2x+1$ and $f(x) = x^4 + 2\omega x^3 - x^2 + 1$ over $\mathbb{Q}(\omega)$. Use Maple's RootOf notation for representing elements of $\mathbb{Q}(\omega)$ and the `gcd` command.

Study the proof of Theorem 8.16 and write out your own version of the proof.

Question 4: Square-free norms.

To factor $f(x)$ over $\mathbb{Q}(\alpha)$, Trager's algorithm chooses $s \in \mathbb{Q}$ such that the norm $N(f(x-s\alpha))$ is square-free. Theorem 8.18 states that only finitely many s do not satisfy this requirement. Give a characterization for which s satisfy this requirement in terms of resultants.
Hint: $n(x)$ is square-free iff $\gcd(n(x), n'(x)) = 1$ where $n(x) = N(f(x - s\alpha))$.

Using your characterization, for $\alpha = \sqrt{2}$ and $f(x) = x^2 - 2$, find all $s \in \mathbb{Q}$ for which the $n(x)$ is not square-free. Repeat this for the factorization problems in question 4.

Question 5: Cyclotomic polynomials.

The n'th cyclotomic polynomial $\Phi_n(x)$ is the minimal polynomial for the primitive n'th root of unity. Devise an algorithm for computing $\Phi_n(x)$ which does not factor $x^n - 1$. Find the first n such that the height (largest coefficient) of $\Phi_n(x)$ is greater than 2.

Note, The Maple command `numtheory[cyclotomic](n,x)` computes $\Phi_n(x)$.
I've computed some of them below.
Note, the Maple command `maxnorm(f)` computes the height of a polynomial.

```
> with(numtheory):
> for n from 1 to 10 do
>     printf("%25a  %50a\n",cyclotomic(n,x),factor(x^n-1));
> od;

                      x-1                                                 x-1
                      x+1                                         (x-1)*(x+1)
                  x^2+x+1                                     (x-1)*(x^2+x+1)
                    x^2+1                                 (x-1)*(x+1)*(x^2+1)
          x^4+x^3+x^2+x+1                             (x-1)*(x^4+x^3+x^2+x+1)
                  x^2-x+1                     (x-1)*(x+1)*(x^2+x+1)*(x^2-x+1)
  x^6+x^5+x^4+x^3+x^2+x+1                     (x-1)*(x^6+x^5+x^4+x^3+x^2+x+1)
                    x^4+1                           (x-1)*(x+1)*(x^2+1)*(x^4+1)
                x^6+x^3+1                           (x-1)*(x^2+x+1)*(x^6+x^3+1)
          x^4-x^3+x^2-x+1     (x-1)*(x+1)*(x^4+x^3+x^2+x+1)*(x^4-x^3+x^2-x+1)
```