Open Questions From AIM Workshop:
The Computational Complexity of Polynomial Factorization

1 Dense Polynomials in $\mathbb{F}_q[x]$

1.1 Open Questions

1. Is there a deterministic algorithm that is polynomial time in n and $\log(q)$?
   State of the art algorithm should be seen on May 16th as a talk.
2. How quickly can we factor $x^2 - a$ without hypotheses (Qi Cheng's question)
   State of the art algorithm Burgess $O(p^{\frac{1}{2e}})$

1.2 Open Question

What is the exponent of the probabilistic complexity (for $q = 2$)?

1.3 Open Question

Given a set of polynomials with very low degree (2 or 3), decide if all of them factor into linear factors. Is it faster to do this by factoring their product or each one individually? (Tanja Lange's question)

2 Sparse Polynomials in $\mathbb{F}_q[x]$

2.1 Open Question

Decide whether a trinomial $x^\alpha + ax^\beta + b$ with $0 < \beta < \alpha \leq q-1$, $a, b \in \mathbb{F}_q$ has a root in $\mathbb{F}_q$, in polynomial time (in $\log(q)$). (Erich Kaltofen's Question)

2.2 Open Questions

1. Finding better certificates for irreducibility
   (a) Are there certificates for irreducibility that one can verify faster than the existing irreducibility tests? (Victor Miller's Question)
   (b) Can you exhibit families of sparse polynomials for which you can find shorter certificates?
2. Find a polynomial-time algorithm in $\log(q)$, where $q = p^n$, that solves $\sum_{i,j=0}^{n-1} a_{i,j} x^{p^i+p^j} + \sum_{i=0}^{n-1} b_i x^{p^i} + c$ in $\mathbb{F}_q$ (or shows no solutions) and works for $\frac{1}{poly}$ of the inputs, and never lies. (We know that this is NP-complete.) (Jintai Ding's Question)

3 Factoring over $\mathbb{Q}[x]$

3.1 Open Question

1. How long does the gradual feeding (or some modification) algorithm actually take to solve one approximate linear equation (with the c_i's bounded by kn bits)? (Mark van Hoeij's Question)

2. (a) Can we do lattice basis reduction in essentially linear time in the total number of digits of the input? (Dan Bernstein's Question)

   (b) Is there a softly linear time reduction from linear system solving to basis reduction in lattices? (Joachim von zur Gathen's question)

3.2 Open Question

Can we use Niederreiter's equation to find a faster algorithm to factor dense polynomials in $\mathbb{Q}[x]$? (Shuhong Gao's Question)

The main possible advantage of such a technique would be to use linear algebra over $\mathbb{F}_p$ instead of lattice basis reduction.

4 Bivariate

4.1 Open Question

For Dense Bivariate polynomials over $\mathbb{F}_p$ with total degree, t: Can we improve on the probabilistic complexity $\tilde{\mathrm{O}}(d^3)$ + Factorization Complexity of Univariate, degree d, polynomial.

Lecerf believes $\tilde{\mathrm{O}}(d^\omega)$ is possible.

The bottleneck is solving d^2 equations in d variables.

4.2 Open Question

Can we find low-degree ($\leq n$) factors of a polynomial with t terms and degree d ($t \ll d^2$, $n \ll d$)

4.3 Open Question

Find an Absolute Factorization (or test for irreducibility) over fields with small ($p < d^2$) characteristic, in $\tilde{\mathrm{O}}(d^3)$.

5 Intermezzo

Given $f \in \mathbb{Q}[x]$ irreducible, and $f(\alpha) = 0$. Factor f over $\mathbb{Q}[\alpha]$.

State of Art: Belabas

6 Numerical

6.1 Open Question

Challenge Problem #1 in Kaltofen's JSC 2000 paper.

6.2 Open Question

Given $f \in \mathbb{C}[x, y]$ find the nearest polynomial that factors into linear factors in $\mathbb{C}[x, y]$.

Find/Bound the distance to the nearest polynomial that factors.

6.3 Open Question

Given $f \in \mathbb{Q}[x, y, z]$, for which values of $z \in \overline{\mathbb{Q}}$ does f factor (completely) in $\mathbb{C}[x, y]$?

What is the degree of a given z?

6.4 Open Question

How to compute/approximate the structured condition number of a Ruppert Matrix.