FINAL EXAM STUDY SUGGESTIONS

The exam will be about double the length of Exam 2 (I’ll aim for 6 pages). It won’t cover everything, only a subset of what I mention below. (In particular, you’ll notice that I’ve omitted discrete log problem and ECDLP, Weil pairings, and Miller-Rabin.)

I will be out of town most of next week, but (assuming no travel issues) will be around Friday afternoon. I plan to hold an office hour for the exam 2-4 on Friday.

Congruences.

• Euler’s theorem: if $(a, n) = 1$, then $a^{\phi(n)} \equiv 1$. (Little Fermat = special case.)
• If $(a, m) = 1$, use Euclidean algorithm to find $b$ such that $ab \equiv 1$. (n)
• Chinese remainder theorem
• Legendre symbols and quadratic reciprocity

Groups, rings and fields.

• Lagrange’s theorem (orders of elements in a group divide the order of the group)
• in a (commutative) ring $R$, meaning of units $R^*$, prime and irreducible elements; unique factorization domain
• ideals in (commutative) rings

Encryption and decryption.

• Diffie-Hellman key exchange
• RSA
• El Gamal
• elliptic Diffie-Hellman
• elliptic El Gamal
Factorization and primality testing.
- Pollard $\rho$ (compositeness test)
- little Fermat: if $(a, n) = 1$, then $a^{n-1} \not\equiv 1 \pmod{n} \implies n$ composite;
  also $a^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n} \implies n$ composite (why?)
- Pollard $p - 1$ method (factoring large $N$)
- Lenstra elliptic method (factoring large $N$, why improvement over Pollard?)

Elliptic curves.
- Group law for $E(\mathbb{C}), E(\mathbb{Q}), E(\mathbb{F}_p)$: draw line through 2 points $P, Q$, take 3rd intersection point; draw line through this point and $o$ (point at $\infty$), 3rd intersection with $E$ defines $P + Q$. Know how to derive the formula for $(x_{P+Q}, y_{P+Q})$ from $(x_P, y_P)$ and $(x_Q, y_Q)$, and for $(x_{2P}, y_{2P})$. (You don’t need to memorize them, but note that knowing something about the formula is crucial to explaining why Lenstra works.)
- How to count number of points $|E(\mathbb{F}_p)|$ using Legendre symbols (formula). Use to compute $E(\mathbb{F}_p)$ as a finite abelian group in simple cases.

Algebraic number rings.
- computing the fundamental unit in a quadratic number ring, and using this to solve Pell-type equations
- definition of algebraic number field $K$ and the ring $\mathcal{O}_K \subset K$ of algebraic integers; fact that $\mathcal{O}_K$ is a UFD (unique factorization domain) $\iff$ $\mathcal{O}_K$ is a PID (principal ideal domain); and that the monoid of integral ideals $\mathcal{I}(K)$ always has unique factorization.
- compute norm, trace, discriminant of elements in a general number field/ring
- the last HW contained a couple of problems on the “ideal norm” and using it to show that certain ideals are non-principal (hence that $\mathcal{O}_K$ is not a PID/UFD)