Math 115 Methods

1. Euclidean Algorithm.
2. Fast Exponentiation (using Fermat's Little Theorem).
3. Calculating $\phi(m)$ (get the prime factorization of m then write $\phi(m) = m(1-\frac{1}{p_1})\dots(1-\frac{1}{p_n})$ where m has n distinct prime factors)
4. Chinese Remainder Theorem.
5. RSA Cryptography (using the Lemma).
6. Hensel's Lemma.
7. Finding a Primitive root modulo m. (if m is prime, then test the positive divisors of $m-1$)
8. Taking Discrete Logarithm (if need to solve $x \equiv 1 \pmod{m}$, then we obtains the following solutions $x \equiv g^a \pmod{m}$ where $a \equiv 0, \frac{\phi(m)}{d}, \frac{2\phi(m)}{d}, \dots, \frac{(d-1)\phi(m)}{d} \pmod{\phi(m)}$)
9. Finding number of primitive roots (if m has a primitive root, there are $\phi(\phi(m))$ of them)
10. Diffie-Hellman Key Exchange.
11. Solving Quadratic Congruences modulo p (make leading coefficient of the polynomial $f(x)$ 1, then complete the square)
12. Manipulation with Legendre/Jacobi symbols.
13. Reducing Binary Quadratic Forms.
14. Writing Finite Simple Continued Fractions (use Euclidean Algorithm).
15. Writing Infinite Simple Continued Fractions (find the part where it repeats, and assign it to be θ and solve the recurrence equation).