Math 115 - Midterm 1 Theorems

1. **Corollary.** Let $a = \prod_p p^{\alpha(p)}$, $b = \prod_p p^{\beta(p)}$, $c = \prod_p p^{\gamma(p)}$.
   (a) $ab = c \iff \alpha(p) + \beta(p) = \gamma(p)\ \forall p$.
   (b) $a \mid c \iff \alpha(p) \leq \gamma(p)\ \forall p$.
   (c) c is a common divisor of a and b iff $\gamma(p) \leq \min(\alpha(p), \beta(p))\ \ \forall p$.
   (d) $\gcd(a, b) = \prod_p p^{\min(\alpha(p),\beta(p))}$.
   (e) $\text{lcm}(a, b) = \prod_p p^{\max(\alpha(p),\beta(p))}$.
   (f) c is the square of an integer iff $\gamma(p)$ is even for all p.
2. **Pascal's Identity.** $\binom{\alpha+1}{k+1} = \binom{\alpha}{k+1} + \binom{\alpha}{k}$.
3. **Binomial Theorem.** $(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$.
4. **Theorem.** If $a \equiv b \pmod{m}$, then $\gcd(a, m) = \gcd(b, m)$.
5. **Euler's Theorem.** If $\gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.
6. **Fermat's Little Theorem.** Let p be a prime. Then:
   (a) $\forall a \in \mathbb{Z}$ and a not a multiple of p, then $a^{p-1} \equiv 1 \pmod{p}$.
   (b) $\forall a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$.
7. **Wilson's Theorem.** If p is prime, then $(p - 1)! \equiv -1 \pmod{p}$.
8. **Solvability of $x^2 \equiv -1 \pmod{p}$.** Let p be a prime. Then, $x^2 \equiv -1 \pmod{p}$ hasa solution $x \in \mathbb{Z}$ iff $p = 2$ or $p \equiv 1 \pmod{4}$.
9. **Fermat's Theorem on Sum of Squares.** Let p be a prime such that $p \equiv 1 \pmod{4}$. Then p can be written as $p = a^2 + b^2$ with $a, b \in \mathbb{Z}$.

10. **Solving Degree 1 Congruences.** Let $a, b \in \mathbb{Z}$ and let $g = \gcd(a, m)$. Then:

    (a) The congruence $ax \equiv b \pmod{m}$ has a solution iff $g \mid b$.

    (b) If (a) is true, then $\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{m}{g}}$ has a solution modulo $\frac{m}{g}$.

11. **Chinese Remainder Theorem.** If $x \equiv a_1 \pmod{m_1}, \ldots, x \equiv a_k \pmod{m_k}$ (where the m_i's are pairwise relatively prime), then let $M = m_1 m_2 \cdot \cdots \cdot m_k$ and $y_i = \text{inverse}\left(\frac{M}{m_i} \pmod{m_i}\right)$. Then, a solution to the simultaneous congruence is given by $x \equiv a_1 \frac{M}{m_1} y_1 + \cdots + a_k \frac{M}{m_k} y_k \pmod{M}$.

12. **Theorem.** If $m \in \mathbb{Z}_{>0}$, then $\phi(m) = \left(\prod_{p \text{ prime}, p \mid m} (1 - \frac{1}{p})\right) \cdot m$.

13. **RSA Cryptography Lemma.** Suppose $m \in \mathbb{Z}_{>0}$ and $\gcd(a, m) = 1$. Let $h, h' \in \mathbb{Z}_{>0}$ such that $hh' \equiv 1 \pmod{\phi(m)}$. Then $a^{kk'} \equiv a \pmod{m}$.

14. **Primality Testing.** If there is an integer a such that $0 < a < m$ and $a^{m-1} \not\equiv 1 \pmod{m}$, then m is not prime.

15. **Hensel's Lemma.** To solve the congruence $f(x) \equiv 0 \pmod{p^k}$, first find the solutions to $f(x) \equiv 0 \pmod{p}$. Then, for each solution a_1 to $f(x) \equiv 0 \pmod{p}$, "lift" its solution by the recurrence relation $a_2 = a_1 - f(a_1)\overline{f'(a_1)}$, where $\overline{f'(a_1)}$ is found by solving $f'(a_1)\overline{f'(a_1)} \equiv 1 \pmod{p}$ for $\overline{f'(a_1)}$. To higher powers, we generalize this recurrence relation to $a_{j+1} = a_j - f(a_j)\overline{f'(a_1)}$.