Number Theory

Figurate Numbers:

Triangular: 1, 3, 6, 10, … $\frac{1}{2}n(n+1)$

Square: 1, 4, 9, 16, … n^2

Pentagonal: 1, 5, 12, 22, 35, … $\frac{1}{2}(3n^2 - n)$

K-gonal: 1, k … $\frac{1}{2}k(n^2 - n) - n^2 + 2n$

Pythagorean triples: These take the form of $M^2 - N^2$, $2MN$, and $M^2 + N^2$. The product of the sides is always divisible by 60.

Primes:

Mersenne: primes of the form $2^p - 1$, where p is a known prime. Not all numbers of this form are prime.

Fermat: primes of the form $2^{2^n} + 1$. The only primes of this form found so far are for $n = 0$ through 4.

Gauss: A regular polygon can only be constructed if the number of vertices is a Fermat prime or the product of distinct Fermat primes.
(Ex. n = 3, 5, or 15 = 3*5). Note: once any n-gon has been constructed, one can easily construct the 2n-gon.

Neighbors of Six: All primes must be in the form $6n+1$ or $6n-1$ (after 2 and 3)

Composite Numbers:

Fundamental Theorem of Arithmetic: every integer greater than 1 has a unique factorization into prime factors.

For an integer n greater than 1, let the prime factorization be $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$

Number of divisors: $d(n) = (e_1 + 1)(e_2 + 1)\cdots(e_k + 1)$

Sum of divisors: $s(n) = \left(\frac{p_1^{e_1+1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{e_2+1} - 1}{p_2 - 1}\right)\cdots\left(\frac{p_n^{e_n+1} - 1}{p_n - 1}\right)$

Any number n such that $d(n)$ is odd is a perfect square.
If $s(n)=2n$, then n is a perfect number.
If $2^p - 1$ is a prime (Mersenne), then $2^{p-1}(2^p - 1)$ is a perfect number.

Congruences:

For any integers a, b, and positive integer m, a is congruent to b modulo m if a – b is divisible by m. This is represented by

$$a \equiv b \pmod{m}$$

This is equivalent to saying a – b = mk for some integer k.

For any integers a, b, c, and positive integers m,

Reflexive property: $a \equiv a \pmod{m}$

Symmetric property: If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

Transitive property: If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$

For any integers a, b, c, d, k, and m, with m > 0, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$:

(i) $a \pm k \equiv b \pm k \pmod{m}$
(ii) $ak \equiv bk \pmod{m}$
(iii) $a \pm c \equiv b \pm d \pmod{m}$
(iv) $ac \equiv bd \pmod{m}$
(v) $a^k \equiv b^k \pmod{m}$

If $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m}$ only if m and c are relatively prime.

Fermat's Little Theorem: For any integer *a* and prime *p*, where *a* and *p* are relatively prime, $a^{p-1} \equiv 1 (\text{mod } p)$.

Wilson's Theorem: An integer *p* is prime if and only if $(p-1)! \equiv -1 (\text{mod } p)$.

Linear Diophantine Equations: The equation $ax + by = c$ has infinitely many solutions for integral *x* and *y* if the greatest common divisor of *a* and *b* divides *c*. If this condition is not satisfied there are no possible solutions.

Divisibility Rules

Let n be represented by the digits $\overline{d}_n\overline{d}_{n-1}\cdots\overline{d}_2\overline{d}_1$. $a \mid b$ means that a divides into b, or that a is a factor of b.

3: A number is divisible by 3 if the sum of its digits is divisible by 3. $3 \mid n$ if $3 \mid \sum_{k=1}^{n} d_k$.

4: A number is divisible by 4 if the number represented by the last two digits is divisible by 4. $4 \mid n$ if $4 \mid 10d_2 + d_1$. This can be reduced to $4 \mid n$ if $4 \mid 2d_2 + d_1$.

6: check for divisibility by both 2 and 3.

8: A number is divisible by 8 if the number represented by the last three digits is divisible by 8. $8 \mid n$ if $8 \mid 100d_3 + 10d_2 + d_1$. More specifically, $8 \mid n$ if $8 \mid 4d_3 + 2d_2 + d_1$.

9: A number is divisble by 9 if the sum of its digits is divisible by 9. $9 \mid n$ if $9 \mid \sum_{k=1}^{n} d_k$.

2^k: A number is divisible by 2^k if the number represented by the last k digits is divisible by 2^k.

7:

Rule 1: Partition n into 3 digit numbers starting from the right ($\overline{d}_3\overline{d}_2\overline{d}_1, \overline{d}_6\overline{d}_5\overline{d}_4, \overline{d}_9\overline{d}_8\overline{d}_7$, etc…) If the alternating sum ($\overline{d}_3\overline{d}_2\overline{d}_1$ - $\overline{d}_6\overline{d}_5\overline{d}_4$ + $\overline{d}_9\overline{d}_8\overline{d}_7$ - …) is divisible by 7, then n is divisible by 7.

Rule 2: Truncate the last digit of n, and subtract twice that digit from the remaining number. If the result is divisible by 7, then n was divisible by 7. This process can be repeated for large numbers.

Ex. n = 228865 $\rightarrow$ 22886 – 2(5) = 22876 $\rightarrow$ 2287 – 2(6) = 2275 $\rightarrow$ 227 – 2(5) = 217 $\rightarrow$ 7 | 217, so 7 | 228865 (228865 = 7*32695)

Rule 3: Partition the number into groups of 6 digits, d_1 through d_6, d_7 through d_{12}, etc. For a 6 digit number n, n is divisible by 7 if ($d_1 + 3d_2 + 2d_2 - d_4 - 3d_5 - 2d_6$) is divisible by 7. For larger numbers, just add the similar sum from the next cycle. The coefficients counting from d_1 are (1, 3, 2, -1, -3, -2, 1, 3, 2, -1, -3, -2, …)

11: A number n is divisible by 11 if the alternating sum of the digits is divisible by 11

$11 \mid n$ if $11 \mid (d_1 - d_2 + d_3 - d_4 + d_5 - \ldots - d_n (-1)^n)$.

13:

Rule 1: See rule 1 for divisibility by 7, n is divisible by 13 if the same specified sum is divisible by 13.

Rule 2: Same process as in rule 3 for 7, the cycle of the coefficients is (1, -3, -4, -1, 3, 4, …)