

Math 104A, Number Theory, Fall 2002.
List of results we have proved during the course.

1. Induction. Proof of formulas and inequalities like $1 + 2 + \cdots + n = n(n + 1)/6$ and $1^2 + 2^2 + \cdots + n^2 = n(n + 1)(2n + 1)/6$ and $n^2 < n!$ for $n > 3$.

2. The binomial coefficients. (a). Defining $\binom{n}{r} = \frac{n!}{r!(n - r)!}$, then

$$(x + y)^n = \binom{n}{0} x^n y^0 + \binom{n}{1} x^{n-1} y + \cdots + \binom{n}{n} x^0 y^n.$$

(b). The binomial coefficients are integers.

(c). If p is prime and $1 \leq r \leq p - 1$ then $p \mid \binom{p}{r}$.

3. Division. Basic properties of divisibility and the division theorem.

4. The floor function (a). Definition of the floor function, basic properties like $\lfloor x + y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor$.

(b). If p is prime, the highest power of p which divides $n!$ is

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots$$

5. There are infinitely many primes of the form $4k + 3$, $3k + 2$, $2^r k + 1$ for r fixed, $2pk + 1$ for a fixed prime p .

6. Greatest common divisor. (a). There exist x and y such that $(a, b) = xa + by$.
(b). If $a \mid bc$ and $(a, b) = 1$ then $a \mid c$.

7. Fundamental Theorem of Arithmetic. Every number greater than 1 is either prime or a product of primes, and the list of primes in the factorization is unique up to reordering.

8. Consequences of the FTA. (a). Formulas for (a, b) and $[a, b]$ in terms of the prime factorizations of a and b leading to results like $a, b = |ab|$.

(b). If n is not a perfect square then \sqrt{n} is irrational.

9. Linear diophantine equations. (a). The equation $ax + by = c$ has a solution (x, y) if and only if $(a, b) \mid c$.

(b). If (x_0, y_0) is a solution to $ax + by = c$ then the general solution is given by $(x, y) = (x_0 + kb/(a, b), y_0 - ka/(a, b))$.

10. Basic properties of congruences. (a). If $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ the $a + b \equiv a' + b' \pmod{m}$ and $ab \equiv a'b' \pmod{m}$ and $a^k \equiv (a')^k \pmod{m}$.

(b). Every integer is congruent modulo m to precisely one element of the standard residue system $\{0, 1, \dots, m - 1\}$. (This is equivalent to the division theorem.)

11. Basic applications of congruences. You can use congruences to answer several questions from Chapter 2 for which you previously used the division theorem. E.g. p.13 #8, p.15 #27, p.37 #8, #9.

12. Inverses Modulo m . The number x has an inverse modulo m if and only if $(x, m) = 1$. The inverse of x is unique modulo m .

13. Linear Congruences. You can solve $ax \equiv b \pmod{m}$ if and only if $(a, m) | b$. Set $d = (a, m)$ then if $d | b$, the solutions of $ax \equiv b \pmod{m}$ are the solutions of $(a/d)x \equiv (b/d) \pmod{m/d}$. Modulo m there are precisely $d = (a, m)$ solutions and if x_0 is one solution then all the solutions modulo m are $x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \dots, x_0 + \frac{(d-1)m}{d}$.

14. Chinese Remainder Theorem.

15. Generalized Chinese Remainder Theorem. Theorem 3.3.4.

16. Polynomial Congruences for prime power moduli. Theorem 3.4.6 (If you know the roots of $f(x) \equiv 0 \pmod{p^k}$ then you can use these to find the roots of $f(x) \equiv 0 \pmod{p^{k+1}}$.)

17. Fermat's Theorem.

18. Application of Fermat's theorem. Proposition 4.1.5: If p is prime and $x^r \equiv 1 \pmod{p}$ then $x^{(r \cdot p-1)} \equiv 1 \pmod{p}$.

19. Euler's Totient Function. If p is prime then $\phi(p^k) = p^k(1 - 1/p)$. If $(m, n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$.

20. Euler's Theorem. The proof uses the following: If $x_1, \dots, x_{\phi(m)}$ are the numbers between 0 and m which are relatively prime to m and $(a, m) = 1$, and y_j is the remainder when ax_j is divided by m , then the list of numbers $y_1, \dots, y_{\phi(m)}$ is just a re-ordering of the list $x_1, \dots, x_{\phi(m)}$.

21. Lagrange's Theorem. We proved an extended version: If $f(x)$ is a polynomial and p is prime then $f(x) = (x - r_1) \cdots (x - r_k)g(x) \pmod{p}$ (poly mod p) where g has no roots modulo p . The roots of f are precisely r_1, \dots, r_k . (The roots may be repeated more than once in this list.) By comparing degrees modulo p , the number of roots modulo p is at most the degree of f .

22. Counting Roots. If p is prime and $d > 0$, the equation $x^d \equiv 1 \pmod{p}$ has precisely $(d, p - 1)$ solutions modulo p . The equation $x^d \equiv -1 \pmod{p}$ has precisely $(2d, p - 1) - (d, p - 1)$ solutions modulo p .

23. RSA. If $n = pq$ where p and q are distinct odd primes, and if $de \equiv 1 \pmod{\phi(n)}$ then $m^{de} \equiv m \pmod{n}$ for $0 \leq m < n$.