Number Theory

Division

1. CRT
2. Multiplicative: $\varphi(n), \tau(n) = |d : d|n|, \sigma(n) = \sum_{d|n} d, \sigma_k(n) = \sum_{d|n} d^k$
3. If f is a multiplicative, so is $g : n \to \sum_{d|n} f(d)$
4. $n = \sum_{d|n} \varphi(d)$; $\varphi(n) = n \prod(1 - 1/p)$
5. Division Algo; Remainder Algo; at most n roots for poly of deg n on integral domain; Lagrange Theorem
6. $(Z/pZ)^\times$ is cyclic [hint: $\sum_{d|p-1} N_d = \sum_{d|p-1} \psi(d) = p - 1$)]
7. $Z/2^k Z$ is not cyclic (homo to $Z/8Z$)
8. $Z/p^k Z$ is cyclic [lemma: if g is a primitive root and $g^{p-1} \neq 1(p^2)$, then g is a generator for $Z/P^k Z$: two possible cases of order of p]

Residue

1. Euler's criteria (prove using Lagrange)
2. Gauss's lemma
3. Jacobi Symbol
4. $(\frac{-1}{n}), (\frac{2}{n})$
5. Quadratic reciprocal for Jacobi ($(x-1)/2 + (y-1)/2 = (xy-1)/2$ mod 2)
6. Jacobi -1 non-square example

BQF

1. integers rep by sum of two square iff p=3 mod 4 to even power (hint: right: consider $\frac{-1}{p}$; left: consider complex modulus, reduce to expressing $p = 1 mod 4$ expressible)
2. BQFs can have the same discriminant but not equivalent; equivalent BQF represents same set of integers
3. Exist BQF with discriminant d iff $d = 0, 1 \mod 4$
4. $(a, b \pm 2a, a \pm b + c)$, $(c, -b, a)$
5. A positive definite BQF is said to be reduced if either $-a < b \leq a < c, or 0 \leq b \leq a = c$
6. Every positive definite BQF is equivalent to a reduced form
7. Reduced: $|b| \leq a \leq \sqrt{|d|/3}, b \equiv d(mod 2)$
8. any $p = 1 mod 4$ is a sum of two squares (hint: $h(-4) = 1 : (1, 0, 1)$; consider $(\frac{-1}{p}) = 1$
9. Properly represent def
10. Least three integers properly represented by a reduced BQF: $a, c, a - |b| + c$
11. Every positive definite BQF is equivalent to a unique reduced form
12. BQF f properly represents n iff f is equivalent to (n, b, c) for some b, c (right: if $f(\alpha, \beta) = n$, Bezout on (α, β), matrix determinant)
13. Let n ∈ N and d < 0 with d ≡ 0, 1 (mod 4), then n is properly represented by some BQF of discriminant d if and only if $x^2 \equiv d(mod 4n)$ is soluble.

Continued Fractions

1. The CFE of θ terminates iff $\theta \in Q$
2. p_n, q_n, a_n
3. $(p_n, q_n) = 1.\ p_n q_{n-1} - q_n p_{n-1} = (-1)^{n+1}$
4. If $\alpha = [a0, \ldots, an, \beta]$ for some $n \geq 0$ and real $\beta > 0$, then $\alpha = (p_n\beta + p_{n-1})/(q_n\beta + q_{n-1})$ and α lies strictly between p_n/q_n and p_{n-1}/q_{n-1}
5. Let $\theta \in R$ be irrational with CFE $[a_0, a_1, \ldots]$. $|\theta - p_n/q_n| < \frac{1}{q_n q_{n+1}}$
6. $p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$
7. Suppose $q \in N$ is such that $1 \leq q < q_{n+1}$ for some n, then for any $p \in Z$ we have $|q\theta - p|$ ≥ $|q_n\theta - p_n|$.
8. Moreover, if $q \in N$ and $p \in Z$ are such that $|\theta - p/q| < |\theta - p_n/q_n|$, then $q > q_n$ use $\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}^{-1}$
9. At least one of any pair of consecutive convergents satisfies $|\theta - p/q| < |\frac{1}{2q^2}|$
10. If $p/q \in Q$ has $|\theta - p/q| < 1/(2q^2)$, then $p/q = p_n/q_n$ for some $n \in N$ $\frac{1}{qq_n} \leq |\frac{p}{q} - \frac{p_n}{q_n}| \leq \cdots$
11. The CFE of an irrational θ is eventually periodic if and only if θ is a quadratic irrational, i.e. the root of a quadratic polynomial with rational coefficents
12. If $d \in N$ is not a square, then $x^2 - dy^2 = 1$ has a solution $(x, y) \in Z^2$ with $xy \neq 0$

Distribution of Primes

1. $\pi(x) \geq logx/(2log2)$
2. $\zeta(s) = X_{n=1}^{\infty} n^s = \prod(1 - 1/p^s)^{-1}$
3. $\mu(n)$
4. $g(n) = \sum_{d|n} f(d) \Rightarrow f(n) = \sum_{e|n} \mu(e) g(\frac{n}{e})$
5. $\zeta(s-1)\zeta(s) = \sum_{N=1}^{\infty} \sigma(N)/N^s$
6. $\zeta\prime(s)/\zeta(s) = -\sum_{n=1}^{\infty} \Lambda(n)/n^s$
7. Legendre formula

Primality Testing

1. Solovay-Strassen Test; An odd composite number $N > 1$ is said to be a Fermat pseudoprime to base b if $(b, N) = 1$ and $b^{N-1} \equiv 1(modN)$

2. If $N$is not a Fermat pseudoprime to some base b_0, then it is not a Fermat pseudoprime to base b for at least half of $b \in (Z/NZ)^\times$

3. Carmichael number (561)

4. Euler pseudoprime

5. Let $N > 1$. If N is not an Euler pseudoprime to some base b_0, then it is not an Euler pseudoprime to at least half the bases in $(Z/NZ)^*$

6. Let $N > 1$. If N is odd and composite, there there is a base $b \in (Z/NZ)^\times$ such that N is not an Euler pseudoprime to base b [hint: square-free/non-square-free case]

7. Miller-Rabin: strong pseudoprime

8. If N is odd and composite, then it passes the strong test for at most a quarter of bases $b \in (Z/NZ)^\times$