List of definitions and theorems and unsolved problems talked about that you should be able to state and possibly prove.

Well Ordering Principle (no proof it’s an axiom, just be able to state)

Principle of Induction (state and be able to prove given an outline)

There are infinitely many primes.

There are arbitrary large gaps between primes.

$\sqrt{2}$ is irrational.

FT of Pascal’s Triangle (state and be able to prove given an outline)

Binomial Theorem (state and be able to prove given an outline)

Division Algorithm (state and be able to prove given an outline)

Theorem 2.2 on page 20. (proofs when asked… all are short exercises)

GCD definition

The GCD of two integers not both 0 can be written as a linear combination of them. $\left(a,b\right)=ax+by$ (be able to prove given an outline)

Two integers are relatively prime iff there is a linear combination of them equal to 1.

(be able to prove given an outline)

Euclidean Algorithm Lemma (state and be able to prove given an outline)

$\left(a,b\right)=1$ iff $1=ax+by$ for some $x$ and $y$(be able to prove given an outline)

Euclid’s Lemma (state and be able to prove given an outline)

$\left(a,b\right)=d$ then $\left(\frac{a}{d},\frac{b}{d}\right)=1$(be able to prove given an outline)

$d$ divides $a$ and $b$ then $d$ divides $ax+by$(be able to prove given an outline)

If $ax+by=c $has a solution $(x\_{0,}y\_{0})$ then all solutions are given by $x=x\_{0}+\left(\frac{b}{d}\right)t$ and $y=y\_{0}+\left(\frac{a}{d}\right)t$ where $\left(a,b\right)=d$ (be able to prove given an outline)

Dirichlet’s Theorem on primes and arithmetic progressions (be able to state)

Prime Number Theorem (be able to state, who proved it and when)

There are infinitely many primes of the form $4n+3$(be able to prove given an outline)

There are infinitely many primes of the form $4n+1$(know that although it seems similar the previous, it is much harder to prove)

If $p$ divides $ab$ then it divides at least one of them. (be able to prove given an outline)

$ax+by=c$ has a sol’n iff $d=(a,b)$ divides $c $(be able to prove given an outline)

Theorem 4.2 all parts are easy exercises.

Definition of $a≡b(n)$.

$a≡b(n)$ iff $a$ and $b$ have the same remainder when divided by $n $(be able to prove given an outline)

Show $ac≡bc(n)$ does not imply $a≡c(n)$.

$ac≡bc(n)$ implies $a≡b\left(\frac{n}{d}\right)$ where $d=\left(c,n\right)$ (be able to prove given an outline)

The Decimal representation of positive integer is unique. (be able to prove given an outline)

$ax≡b(n)$ has solutions iff $d=\left(a,n\right)$ divides $b. $(be able to prove given an outline)

If $ax≡b(n)$ has solutions then it has $d=\left(a,n\right)$ distinct solutions mod $n. $(be able to prove given an outline)

Chinese Remainder Theorem (be able to state and prove given outline)

$a$ and $b$ each dividing $c$ with $\left(a,b\right)=1$ implies $ab$ divides $c $(be able to prove given an outline)

Fermat’s Little Theorem(be able to state and prove given outline)

Definition of pseudoprime. Smallest is ?

Definition of Carmichael Number. Smallest is ?

$n$ odd pseudoprime implies $M=2^{n}-1$ is also. (be able to prove given an outline)

Wilson’s Theorem (be able to state and prove given outline)

Converse of Wilson’s Theorem (be able to prove given an outline)

Show $2^{340}≡1(341)$ hint factor 341 do it modulo each of it’s factors.

Show $a^{560}≡1(561)$ hint factor 561 do it modulo each of it’s factors.

Definition of $τ(n)$ and $σ\left(n\right).$

The divisors of $n=p\_{1}^{k\_{1}}p\_{2}^{k\_{2}}…p\_{r}^{k\_{r}}$ are of $p\_{1}^{a\_{1}}p\_{2}^{a\_{2}}…p\_{r}^{a\_{r}}$ where $0\leq a\_{i}\leq k\_{i}$ (be able to prove given an outline).

$a+ar+ar^{2}+…+ar^{n}=\frac{ar^{n+1}-a}{r-1}$. (be able to prove given an outline).

Let $n=p\_{1}^{k\_{1}}p\_{2}^{k\_{2}}…p\_{r}^{k\_{r}}$ then $τ\left(n\right)=\left(k\_{1}+1\right)\left(k\_{2}+1\right)…(k\_{r}+1)$ and $σ\left(n\right)=\frac{p\_{1}^{k\_{1}+1}-1}{p\_{1}-1}\frac{p\_{2}^{k\_{2}+1}-1}{p\_{2}-1}…\frac{p\_{r}^{k\_{r}+1}-1}{p\_{r}-1}$. (be able to prove given an outline)

It is the case that $n^{\frac{τ(n)}{2}}=\prod\_{d|n}^{}d$ (be able to prove given an outline)

Definition of a multiplicative number-theoretic function.

$τ\left(n\right)$ and $σ(n)$ are multiplicative. (be able to prove given an outline)

Let $\left(m,n\right)=1$ then the divisors of $mn$ are of the form $de$ where $d$ divides $m$ and $e$ divides $n$, and these products are all distinct and $\left(d,e\right)=1.$ (be able to prove given an outline)

If $f$ is multiplicative the so is $F\left(n\right)=\sum\_{c|n}^{}f(c).$ (be able to prove given an outline)

Mobius Inversion Formula Definition.

$μ\left(n\right)$ is multiplicative.(be able to prove given an outline)

$F\left(n\right)=\sum\_{d|n}^{}μ(d)=\left\{\begin{array}{c}1 if n=1\\0 if n>1\end{array}\right.$. (be able to prove given an outline)

Let $F\left(n\right)=\sum\_{d|n}^{}f(d)$ then $f\left(n\right)=\sum\_{d|n}^{}μ\left(d\right)F\left(\frac{n}{d}\right)=\sum\_{d|n}^{}μ\left(\frac{n}{d}\right)F\left(d\right)$ (MOBIUS INVERSION FORMULA) (be able to state and prove given outline)

If $F\left(n\right)=\sum\_{c|n}^{}f(c) $is multiplicative so is $f.$ (be able to prove given an outline)

Definition of Euler’s Phi-Function.

$φ\left(p^{k}\right)=p^{k}-p^{k-1}=p^{k-1}\left(1-\frac{1}{p}\right)$. (be able to prove given an outline)

$\left(a,bc\right)=1 $iff $\left(a,b\right)=1 $and $\left(a,c\right)=1.$(be able to prove given an outline)

The Euler Phi-Function is multiplicative.$ $(be able to prove given an outline)

 Formula for $φ(n=p\_{1}^{k\_{1}}p\_{2}^{k\_{2}}…p\_{r}^{k\_{r}})$ (be able to prove given an outline)

Euler’s Theorem (be able to state and prove given outline)

The sum of the numbers less than $n$, relatively prime to $n$ is $\frac{n}{2}φ(n)$ (be able to prove given an outline)