(We marked page numbers based on the textbook, “Fundamentals of Number Theory” written by Willam J. Leveque.)

Chapter 1

p. 5

primepi(x) : the number of prime numbers that are less than or equal to x (= $=\pi(x)$

```
------------------------------
? primepi(10)
%1 = 4
? primepi(10^3)
%2 = 168
? primepi(10^10)
%3 = 455052511
------------------------------
```

p. 7

numdiv(x) : the number of divisors of x (= $\tau(x)$)

```
--------------------------------
? numdiv(12)
%1 = 4
--------------------------------
```

Remind that 12 has 6 divisors: 1,2,3,4,6, and 12.

Programming)

For example, you may construct a table of values of $\tau(n)$ for $1 \leq n \leq 5$ as follows:

```
---------------------------------------
? for(j=1,5,print(“t(”,j,"):”,numdiv(j)))
t(1):1
t(2):2
t(3):2
t(4):3
t(5):2
---------------------------------------
```

p. 19 division algorithm

a\/b : returns quotient q where $a=bq+r,\ 0 \leqq r < |q|$.

a\b and a%b : return quotient q and remainder r respectively where $a=bq+r$, $0 \leqq r < q$.

divrem(x,y) : returns the quotient a\b and remainder a%b in the form of column matrix.

```
-----------------------
gp > -7 \/ 3
%1 = -2

gp > -7 \ 3
%2 = -3

gp > -7 % 3
%3 = 2

gp > divrem(x,y)
%4 = [-3, 2]~
-----------------------
```

Recall that -7 =3*(-2)+(-1) = 3*(-3)+2.

p. 21

factor(x) : factorization of x

```
? factor(12)
-----------------------
%1 =
[2 2]
[3 1]
-----------------------
```

For each row vector of the result, the first entry is the prime number that divides x, and the second is its exponent.

P.24

sigma(x, k) : the sum of k-th powers of the positive divisors of $|x|$. For example, simga$(12,3) = 1^3+2^3+3^3+4^3+6^3+12^3 = 2044$.

```
---------------------------------------
gp > sigma(6, 1)
%1 = 12
---------------------------------------
```

Chapter 2

p.32

gcd(x, y) : finds the greatest common divisor of x and y.

```
----------------------
gp > gcd(15, 21)
%1 = 3
----------------------
```

p.33

bezout(x,y) finds [u, v, d] such that x*u + y*v = d where d is the greastest common divisor of x and y.

```
-----------------------------------
gp > bezout(123, 54)
%1 = [-7, 16, 3]

gp > bezout(47, 91)
%2 = [31, -16, 1]
-----------------------------------
```

p.35 Problem14

Programming)
Write program for the Euclidean algorithm.

```
-------------------------------------------------------------------------------
>EucAlg(m,n)=local(a,b,r);if(abs(m)>=abs(n),{a=m;b=n;},{a=n;b=m;});r=a%b;;while(r!=0,
print(a,"=",b,"*",a\b,"+",r);a=b;b=r;r=a%b;);if(r==0,print(a,"=",b,"*",a\b));
-------------------------------------------------------------------------------
```

Then you type

```
> EucAlg(741,715)
```

and compare the result to the equations on p.32. The result should be

```
---------------------------------
741 =715*1+26
715=26*27+13
```

```
26=13*2
---------------------------------
```

It is easy to check that underlined 13 on the last line is the gcd of 741 and 715.

The program for the least remainder algorithm is left for the readers.

p.44

lcm(x, y) : finds the least common multiplier of x and y.

```
----------------------
gp >lcm(14, 35)
%1 = 70)
----------------------
```

Chapter 3

p.53

eulerphi(n) : computes the Euler phi function $\phi(n)$.

```
-----------------------------------------------
gp > eulerphi(17)
%1 = 16
gp > eulerphi(36)
%2 = 12
-----------------------------------------------
```

p.62 Problem 1

To find solutions of the system of linear modular equations, we may use the Chinese Remainder Theorem. Suppose we have the following system of linear modular equations:

$$x \equiv 3 \pmod{4}$$
$$x \equiv 5 \pmod{21}$$
$$x \equiv 7 \pmod{25}.$$

To solve this system, we type

```
-------------------------------------------
chinese(chinese(Mod(3,4),Mod(5,21)),Mod(7,25))
%1 = Mod(1307,2100)
-------------------------------------------
```

To be precise, chinese(Mod(3,4),Mod(5,21)) returns Mod(47,84) which means $x \equiv 47 \pmod{84}$ is the solution of two modular equations

$$x \equiv 3 \pmod{4}$$
$$x \equiv 5 \pmod{21}.$$

X. Primitive root P.79

znprimeroot(x) calculates a primitive root of x, where x is a power of a prime.
If p is a prime and g is a primitive root mod p, then znlog(x, g) returns the discrete logarithm of x (to the base g) in $\mathbb{Z}/p\mathbb{Z}$.

For example, 3 is a primitive root mod 17, and we have

$3^0 = 1,\ 3^1 = 3,\ 3^2 = 9,\ 3^3 = 10,\ 3^4 = 13,\ 3^5 = 5,\ 3^{6=15},\ 3^{7=11},\ 3^{8=16}$
$3^9 = 14,\ 3^{10=}8,\ 3^{11} = 7,\ 3^{12} = 4,\ 3^{13} = 12,\ 3^{14} = 2,\ 3^{15} = 6,\ 3^{16} = 1$

Thus the discrete logs mod 17 (to the base 3) are

$\log = 0,\ \log 2 = 14,\ \log 3 = 1,\ \log 4 = 12,\ \log 5 = 5,\ \log 6 = 15,\ \log 7 = 11,\ \log 8 = 10$
$\log 9 = 2,\ \log 10 = 3,\ \log 11 = 7,\ \log 12 = 13,\ \log 13 = 4,\ \log 14 = 9,\ \log 15 = 6,\ \log 16 = 8$

```
------------------------------
gp > znprimroot(17)
%1 = Mod(3, 17)

gp > znlog(2, znprimroot(17))
%2 = 14
gp > znlog(11, znprimroot(17))
%3 = 7
gp > znlog(14, Mod(3,17))
%4 = 9
------------------------------
```

Chapter 5

p.109

kronecker(x,y) : returns the Legendre symbol (or its generalization, Jacobi symbol) (x/y).

```
gp > kronecker(2, 17)
%1 = 1

gp > kronecker(14, 17)
%1 = -1
```

It indicates that 2 is a quadratic residue modulo 17, but 14 is not.

To check the multiplicative of Jacobi symbol,

```
gp > kronecker(2, 21)
%1 = -1

gp > kronecker(2,3)
%2 = -1

gp > kronecker(2,7)
%3 = 1
```

Chapter 6

P.125

sumdiv(x, X, f(X)) sums $f(X)$ over all positive divisors of n. Note that sumdiv(x,X,X^k) is same as sigma(x,k), but computation of sigma(x,k) is much faster because it takes advantages of the multiplicativity of x^k.

```
---------------------------
gp > sumdiv(6,X,X)
%1 = 12
gp > sumdiv(6,X,X^3)
%2 = 2044
---------------------------
```

P.127

moebius(n) : Moebius function $\mu(n)=0$ if n contains a repeated prime factor, else $\mu(1)=1$ and $\mu(n)=(-1)^k$, where k is the number of distinct prime factors of n.

```
-----------------
gp > moebius(12)
%1 = 0
gp > moebius(6)
%2 = 1
gp > moebius(30)
%3 = -1
-----------------
```

P.154

zeta(s) is the Riemann zeta function.

```
-------------------------------------------------
gp > zeta(1)
*** at top-level: zeta(1)
***                ^------
*** zeta: domain error in zeta: argument = 1

gp > zeta(2)
%1 = 1.6449340668482264364724151666460251892
```

```
gp > zeta(0)
%2 = -0.50000000000000000000000000000000000000
------------------------------------------------
```

Chapter 8

P.198 (Pell's equation)

The instruction contfrac(x, l) will give an approximation to x based on l convergents. For example, contfrac(41/18, 3) returns [2,4], which is the same as [2,3,1]

The continued fraction expansion of an irrational number is infinite, but when the irrational number is $\sqrt{N}$, there are very useful properties of periodicity and symmetry. We will illustrate with an example. The continued fraction of $\sqrt{N}$ is

$$\sqrt{21} = 4,\overline{1,1,2,1,1,8} = [4,1,1,2,1,1,8,1,1,2,1,1,8,1,1,2,1,1,8,...].$$

The general pattern is

$$[a_0,a_1,...,a_n,2a_0,a_1,...,a_n,2a_0,a_1,...,a_n,2a_0,...]$$

where the segment $a_1,...,a_n$ is symmetric about its midpoint. If n is odd, then the n-th convergent gives a minimal solution of Pell's equation. In our case, $n=5$, and the command contfracpnqn([4,1,1,2,1,1]) returns $p_n/q_n = 55/12$. Indeed, we have

$$p_n^2 - Nq_n^2 = (55)^2 - 21(12)^2 = 3025 - 3024 = 1.$$

```
---------------------------------
gp > contfracpnqn([4,1,1,2,1,1])
%1 =
[55 32]
[12 7]
---------------------------------
```

More on Continued Fraction

contfrac(x,{b},{nmax}) returns contined fraction expansion of x. nmax is a bound for the number of terms of the result.

Here, {b} = [b_0,b_1,cdots,b_n] represents the vector of numerators of the continued fraction.

contfrac(x,{[b_0,cdots,b_n},{nmax}) = [a_1,a_2,⋯,a_{nmax}] means, in fact,

$$\begin{cases} \text{if } b_0 \neq 0,\ x \cdot b_0 = a_1 + \dfrac{b_1}{a_2 +}\dfrac{b_2}{a_2 +}\cdots \\ \text{if } b_0 = 0,\ x = a_1 + \dfrac{b_1}{a_2 +}\dfrac{b_2}{a_2 +}\cdots . \end{cases}$$

```
gp > contfrac(sqrt(2)-1,6)

%1 = [0, 2, 2, 2, 2, 2]

gp > contfrac(19/17,[2,3,3],3)

%2 = [2, 12, 4]
```

Caution1 : If input {b} is an integer b, then {nmax} will be ignored and the commnad contfrac(x, b, nmax) evaluates contfrac(x,b)

Caution2 : contfrac command is indeed unstable because its output may not be the one that we do not expect at all. For example,

contfrac(Pi,4) outputs [3,7,16]. Because Pi is irrational, contfrac(Pi, n) must output a row-vector of n entries. Another example is the above explanation of the command itself.

Appendix

PARI Types & Input Formats

In GP, you do not need to define the types of variables you are going to use. (e.g. int a; or double b; are not neccessary.)

Moreover, some binary operations in GP works properly even if the types of inputs are different.
(See, for example, t_INTMOD. Note that 4+5 = 2 mod 7)

The followings are typical types of objects in GP. If GP outputs an error code, this table may be helpful.

Type	Description Example
t_INT	Integers(It may be decimal, hexadecimal, or binary.) ---------- gp > a=0x1F %1 = 31 gp > b=0b101 %2 = 5 gp > a+b %3 = 36 ----------
t_REAL	Real numbers. To represents rational number $\frac{a}{b}$ in binary, you may add dot to the numerator(Input a./b). 31.4, 5.27 E4, 1./3
t_INTMOD	Integers modulo m ---------- gp > a=Mod(4,7) %1 = Mod(4,7) gp > a+5 %2 = Mod(2,7) ----------
t_FRAC	Rational Numbers. Note here that a/b is of type t_FRAC iff a and b are of type t_INT. GP operates suitably so that a/b may be translated to $a*b^{-1}$) Mod m if a is of type t_INT and b is of type t_INTMOD(or t_FFELT). Furthermore, unlike MATLAB or so on, 1/3 does not mean $0.333\cdots$.

	GP really reads 1/3 as a rational number "$\frac{1}{3}$".
t_FFELT	Element in finiite field GF(q). q may not be prime.
	5+ffgen(13)
t_COMPLEX	Complex Numumbers. I:=sqrt(-1). Do not forget to use *
	3+sqrt(10)*I
t_POLMOD	Polynomials modulo g. The behavior of t_POLMOD varible is similar to the one of t_INTMOD.
	Mod(f,g)
t_POL	Polynomaials. Do not forget to use * to represent multiplication of coefficient.
t_VEC/t_COL	Row/Column Vectors. "~" represents transpose operation.
	[x,y,z]/[x,y,z]~
t_MAT	Matrices. Each row-vectors are divided by semi-colon.
	[a,b;c,d]