Solutions to Homework Assignment 1
CS 6104: Algorithmic Number Theory

Problem 1. **[Solution courtesy of Nick Loehr]** Use the techniques in Chapter 2 to derive an asymptotic estimate for

$$h(x,k) \;=\; \sum_{p\le x} p^k,$$

where $k \geq 1$ is an integer. For $k \in \{1,2,3,4\}$ and $x \in \{10,50,100,200\}$, use *Mathematica* to compute $h(x,k)$ precisely. Present these results in a table along with the values of your asymptotic estimates.

Recall Theorem 2.7.1, which states that for continuously differentiable functions g,

$$\sum_{p\le x} g(p) = \int_2^x \frac{g(t)\,dt}{\log t} + \epsilon(x)g(x) - \int_2^x \epsilon(t)g'(t)\,dt. \tag{1}$$

where $\epsilon(x) = o(x/\log x)$. Fix an integer $k \geq 1$, and set $g(x) = x^k$. Then (1) becomes:

$$h(x,k) = \sum_{p\le x} p^k = \int_2^x \frac{t^k\,dt}{\log t} + \epsilon(x)x^k - \int_2^x kt^{k-1}\epsilon(t)\,dt. \tag{2}$$

First, let us estimate the integral $\int_2^x \frac{t^k\,dt}{\log t}$. We will use Theorem 2.6.1 with $f(x) = x^k/(\log x)$. We have

$$\frac{f'(x)}{f(x)} = \frac{(kx^{k-1}\log x - x^{k-1})/(\log^2 x)}{x^k/(\log x)} = \frac{k\log x - 1}{x\log x} = \frac{k}{x} - \frac{1}{x\log x} \sim \frac{k}{x}.$$

We may take $\mu = k$ in the theorem. Since $k \neq 0$, we obtain

$$\int_2^x \frac{t^k\,dt}{\log t} \sim \frac{xf(x)}{\mu+1} = \frac{x^{k+1}}{(k+1)\log x}.$$

Knowing that $\epsilon(x) = o(x/\log x)$, it's obvious that the two error terms $\epsilon(x)x^k$ and $\int_2^x kt^{k-1}\epsilon(t)\,dt$ are each $o(x^{k+1}/\log x)$. Hence, we have

$$h(x,k) \sim \frac{x^{k+1}}{(k+1)\log x}.$$

The following *Mathematica* code computes $h(x,k)$ precisely for the given values of x and k:

```
In[1]:= h[x_,k_] := Module[
          {sum, i},
          sum=0; i=2;
          While[ i <= x,
            If[ PrimeQ[i], sum = sum + i^k, ];
            i = i + 1
```

```
          ];
          sum]
In[11]:= Table[h[10,k],{k,1,4}]
In[12]:= Table[h[50,k],{k,1,4}]
In[13]:= Table[h[100,k],{k,1,4}]
In[14]:= Table[h[200,k],{k,1,4}]
```

The following code computes approximations for $h(x,k)$ using the formula just derived:

```
n[18]:= ah[x_,k_]:=N[x^(k+1)/((k+1)*Log[x])]
In[19]:= Table[ah[10,k],{k,1,4}]
In[20]:= Table[ah[50,k],{k,1,4}]
In[21]:= Table[ah[100,k],{k,1,4}]
In[22]:= Table[ah[200,k],{k,1,4}]
```

The *exact* results produced by *Mathematica* are as follows.

x	$h(x,1)$	$h(x,2)$	$h(x,3)$	$h(x,4)$
10	17	87	503	3123
50	328	10466	385054	15169214
100	1060	65796	4696450	360663864
200	4227	565065	86470593	14185215405

The *approximations* produced by *Mathematica* are as follows.

x	$h(x,1)$	$h(x,2)$	$h(x,3)$	$h(x,4)$
10	21.7147	144.765	1085.74	8685.89
50	319.528	10650.9	399410	1.59764×10^7
100	1085.74	72382.4	5.42868×10^6	4.34294×10^8
200	3774.78	503304	7.54957×10^7	1.20793×10^{10}

Problem 2. [Solution courtesy of Nick Loehr] Let R be the ring $\mathbb{Z}/(3)$, and consider the polynomial ring $R[X]$. Let $f \in R[X]$ be the polynomial

$$f(X) \quad = \quad X^2 + 3X + 2.$$

Finally, let

$$I \quad = \quad \{g(X)f(X)h(X) \mid g, h \in R[X]\}.$$

A. Prove that I is an ideal in $R[X]$.

B. Let $T = R[X]/I$. How many elements does T have? What are they?

C. Give addition and multiplication tables for T.

D. Is T a field? Why or why not?

A. Let $J = \{p(x)f(x) \mid p \in R[x]\}$. We claim that $I = J$. To see this, take any $p \in R[x]$. Letting $g = p$ and $h = 1$ in the definition of I shows that $J \subset I$. Similarly, for any $g, h \in R[x]$, note that $g(x)f(x)h(x) = (g(x)h(x))f(x)$. Taking $p(x) = g(x)h(x)$ shows that $I \subset J$.

The proof that I is an ideal is now identical to the proof given in class that J is an ideal. We repeat that proof here for completeness.

Certainly $0 \in J$, so J is non-empty.

Suppose $p_1(x)f(x)$ and $p_2(x)f(x)$ are arbitrary elements in J. Then

$$p_1(x)f(x) + p_2(x)f(x) = (p_1(x) + p_2(x))f(x) \in J,$$

using the distributive law and the fact that $p_1(x) + p_2(x) \in R[x]$. So J is closed under addition.

Similarly, if $p(x)f(x) \in J$ and $q(x) \in R[x]$, then

$$q(x)[p(x)f(x)] = [q(x)p(x)]f(x) \in J,$$

using the associativity of multiplication and the fact that $q(x)p(x) \in R[x]$. So J is closed under multiplication by elements of $R[x]$. Hence, $J = I$ is an ideal in $R[x]$.

B. The factor ring T has nine elements, namely the equivalence classes

$$\{\overline{0}, \overline{1}, \overline{2}, \overline{x}, \overline{x+1}, \overline{x+2}, \overline{2x}, \overline{2x+1}, \overline{2x+2}\}.$$

To see that these nine elements are distinct, observe that I consists of all multiples of $f(x) = x^2 + 2$. Nonzero multiples of I will clearly have degree at least 2, since the coefficient ring $\mathbb{Z}/(3)$ has no zero divisors. Thus, the difference of two distinct elements of the form $a_0 + a_1 x$ is not in I, since this difference is a nonzero polynomial of degree less than 2.

Next, T does not have any additional elements. For, any polynomial of degree 2 or more is equivalent to one of the polynomials listed above, since we can reduce modulo f to replace x^2 by $-2 = 1$, x^3 by x, etc.

C. The addition table for T is as follows: (Here, we write 0 for the equivalence class $\overline{0}$, etc.)

$+$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

This first table is easily computed by noting that $3 = 0$ in the coefficient ring.

The multiplication table for T is easily computed if we remember to replace x^2 by 1 whenever it appears in a product. We get:

$*$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	1	$x+1$	$2x+1$	2	$x+2$	$2x+2$
$x+1$	0	$x+1$	$2x+2$	$x+1$	$2x+2$	0	$2x+2$	0	$x+1$
$x+2$	0	$x+2$	$2x+1$	$2x+1$	0	$x+2$	$x+2$	$2x+1$	0
$2x$	0	$2x$	x	2	$2x+2$	$x+2$	1	$2x+1$	$x+1$
$2x+1$	0	$2x+1$	$x+2$	$x+2$	0	$2x+1$	$2x+1$	$x+2$	0
$2x+2$	0	$2x+2$	$x+1$	$2x+2$	$x+1$	0	$x+1$	0	$2x+2$

D. T is *not* a field since not all nonzero elements have multiplicative inverses. For example, $x+1$ has no multiplicative inverse, by inspection of the table above.

Problem 3. [Solution courtesy of Jeremy Rotter] Chapter 3, Problem 8.

A. Give pseudocode for your algorithm to solve $f(x) = n$. Analyze its worst case time complexity.

B. Program your algorithm in *Mathematica* or other symbolic computation system. Include the *Mathematica* code in your solution.

C. Use your algorithm to determine whether a solution exists to

$$f(x) = 331104019746398614665567837536000231540518038885870489393 00,$$

where $f(x)$ is this polynomial

$$14x^{17} + 99x^7 + 3x^2 + 94.$$

A. The following is pseudocode for an algorithm which will determine whether there exists a positive integer x such that $f(x) = n$, and if there is, it will return that integer. Otherwise it will return `FALSE`.

The problem specification did not require a proof on why this works, so I haven't provided one! In a nutshell, however, this algorithm works because when $x > 0$, $f'(x) \geq 0$. This means that when $x > 0$, the function is increasing, and hence we can rely on the fact that, if $f(a) < n$, then $f(x) < n$ for all $0 \leq x \leq a$. Similarly, if $f(a) > n$, then $f(x) > n$ for all $x \geq a$. This allows us to use a binary search to find the solution.

DiophantineSolve(input: Diophantine function f, positive integer n)

// Set the range of integers in which we will find our answer
$rbegin \leftarrow 0$
$rend \leftarrow n$

// Choose our initial guess
$index \leftarrow \lfloor \frac{rend+rbegin}{2} \rfloor$
$val \leftarrow f(index)$

// Search until we find an answer or run out of integers
while $(rbegin \neq rend)$ **and** $(val \neq n)$

// If the search range was of length 1, make it length 0
if $(rend - rbegin) = 1$
then $rbegin \leftarrow rend$
else if $(val > n)$
then $rend \leftarrow (index - 1)$
else $rbegin \leftarrow (index + 1)$
$index \leftarrow \lfloor \frac{rend+rbegin}{2} \rfloor$
$val = f(index)$

if $(val \neq n)$
then return `FALSE`
else return *index*

This algorithm, in the worst case, is clearly $O(\log_2 n)$, since all it does is start with a search range of $[0, n]$, and then it uses a binary search to repeatedly half the range until it either finds an x such that $f(x) = n$ or it reduces the search range to a single integer. Everything outside of the while loop in the program will run in constant time. The $O(\log_2 n)$ represents the worst case number of calls to the function f, which I am assuming also runs in a constant amount of time.

B. The following is the *Mathematica* code to solve $f(x) = n$:

```
(**********************************************************************
 Function DiophantineSolve takes as parameters a function f and an
   integer n, and returns either a non-negative integer x such that
   f(x) = n or -1 if no such non-negative integer exists.
**********************************************************************)

DiophantineSolve[f_, n_] := Module[{},

    (* Set the range of integers in which we will find our answer *)
```

```
    rbegin = 0;
    rend = n;

    (* Choose our initial guess *)
    index = Floor[(rend+rbegin)/2];
    val = f[index];

    (* Search until we find an answer or run out of integers *)
    While[(rbegin != rend)&&(val != n),

        (* If the search range was of length 1, make it length 0 *)
        If[(rend-rbegin) == 1, rbegin = rend,
            If[ val > n, rend = index - 1, rbegin = index + 1]
        ];
        index = Floor[(rend+rbegin)/2];
        val = f[index];
    ];

    (* Set -1 as the return value if no answer was found *)
    If[ val != n, index = -1];
    index
]
```

C. Here are the commands I gave to *Mathematica* to find the solution for the given n:

```
(* Here we define f *)
f[x_] := 14x^17 + 99x^7 + 3x^2 + 94

(* Now we can solve part C on the homework *)
DiophantineSolve[f, 33110401974639861466556783753600023154051803888587048939300]
```

The *Mathematica* function found the solution:

$$f(2371) = 33110401974639861466556783753600023154051803888587048939300.$$