Introduction to Number Theory
Tutorial 1

Stephen Burke, Adam Keilthy, Marianna Kelly,
Katarina Manojlović, Aisling Mullins

27.1.14

1 Question 1

To find $a_0 + a_1 + ... + a_k$ such that $a_0 + a_1 m^2 + ... + a_k m^k$ proceed as follows:

$n = q_0 m + a_0$
$q_0 = q_1 m + a_1$
$\vdots$
$q_{k-1} = q_{k-1} + a_k$
$q_k = q_{k+1} m + 0 = 0$ (as $a_{k+1} = a_{k+2} = ... = 0$)
The a_i are the remainders obtained on repeated division by m.

$$\begin{aligned}\Rightarrow \sigma_m(n) &= a_0 + ... + a_k \\ &= n - q_0 m + q_0 - q_1 m + ... + q_{k-1} \\ &= n - q_0(m-1) + q_1(m-1) + ... + q_{k-1}(m-1) \\ &= n - Q(m-1) \text{ , } Q = q_0 + ... + q_{k-1}\end{aligned}$$
$$\Rightarrow n - \sigma_m(n) = n - (n - Q(m-1)) = Q(m-1)$$

$\therefore (m-1)$ divides $n - \sigma_m(n)$

Alternatively note that $n - \sigma_m(n) = a_1(m-1) + a_2(m^2-1) + ... + a_k(m^k - 1)$
As $m^i - 1 = (m-1)(m^{i-1} + m^{i-2} + ... + m + 1)$ it is clear that $(m-1)$ divides $n - \sigma_m(n)$

2 Question 2

Base case: n=1:

In base p, 1=1 so $\sigma_p(1) = 1$

$\Rightarrow \frac{n-\sigma_p(n)}{p-1} = \frac{1-1}{p-1} = 0$, which is true, as $p \nmid 1! = 1$

Suppose this is true for n.

Denote by $o_p(n)$ the highest power of p dividing n.

Then it is clear that $o_p(ab) = o_p(a) + o_p(b)$

Proof: Let $a = p^\alpha q$, $b = p^\beta r \Rightarrow ab = p^{\alpha+\beta} qr$, $p \nmid q,r$

Then $o_p(ab) = o_p(p^{\alpha+\beta} qr) = \alpha + \beta = o_p(a) + o_p(b)$

Hence, $o_p((n+1)!) = o_p(n+1) + o_p(n!)$

$= o_p(n+1) + \frac{n-\sigma_p(n)}{p-1}$

Let $a_0 + ... + a_k p^k$ be the base p expansion of n

If $a_0 \neq p-1$ then n+1 is not divisible by p, $\sigma_p(n+1) = \sigma_p(n) + 1$ and so $\frac{(n+1)-\sigma_p(n+1)}{p-1} = \frac{n-\sigma_p(n)+1-1}{p-1} = \frac{n-\sigma_p(n)}{p-1}$

$o_p(n+1) = 0 \Rightarrow o_p((n+1)!) = o_p(n!) = \frac{n-\sigma_p(n)}{p-1} = \frac{(n+1)-\sigma_p(n+1)}{p-1}$

If $a_0 = p-1 \Rightarrow p \mid n+1$. Let $r = o_p(n+1)$

Then the base p expansion of n+1 is:

$b_r p^r + b_r p^{r+1} + ... + b_k p^k + b_{k+1} p^{k+1} = 1 + a_0 + a_1 p + ... + a_k p^k + a_{k+1} p^{k+1}$

$\Rightarrow b_r = a_r + 1$, $b_{r+1} = a_{r+i}$ $(a_0 = ... = a_{r+i} = p-1)$ $\forall i = 1, ..., k+1 = r$,
as this expansion is unique.

$\Rightarrow \sigma_p(n+1) = 1 + a_r + ... + a_{k+1} = \sigma_p(n) + 1 - \sum_{i=1}^{r-1} a_i$

$\Rightarrow \frac{n+1-\sigma_p(n+1)}{p-1} = \frac{n-\sigma_p(n)}{p-1} + \frac{\sum_{i=1}^{r-1} a_i}{p-1}$

$= \frac{n-\sigma_p(n)}{p-1} + \frac{r(p-1)}{p-1} = \frac{n-\sigma_p(n)}{p-1} + r$

$\Rightarrow o_p(n+1) + \frac{n-\sigma_p(n)}{p-1} = r + \frac{n-\sigma(n+1)}{p-1}$

$o_p((n+1)!) = \frac{(n+1)-\sigma_p(n+1)}{p-1}$

Hence, by induction, we are done.

3 Question 3

Let $n_1 = a_0 + a_1 p + ... + a_k p^k$ and $n_2 = b_0 + b_1 p + ... + b_k p^k$ and suppose $l \geq k$

$\Rightarrow n_1 + n_2 = (a_0 + b_0) + ... + (a_k + b_k)p^k + ... + b_l p^l$
$= c_0 + c_1 p + ... + c_l p^l$, $0 \leq c_1 < p$

We have either:

- $a_i + b_i = c_i \Rightarrow a_i + b_i - c_i = 0$
- $a_i + b_i = c_i + p \Rightarrow a_i + b_i - c_i = p$ (Leads to carrying)
- $a_i + b_i + 1 = c_i + p \Rightarrow a_i + b_i - c_i = p - 1$ (Leads to carrying & implies carrying has occured.)
- $a_i + b_i + 1 = c_i \Rightarrow a_i + b_i - c_i = -1$ (Implies carrying has occured.)

$\Rightarrow \sigma_p(n_1) + \sigma_p(n_2) - \sigma_p(n_1 + n_2) = Ap + B(p-1) + C(-1)$
Where A is the number of times $a_i + b_i = c_i + p$ etc.

$\Rightarrow A + B =$ number of times we carry $= B + C$
$\Rightarrow A = C$

$\Rightarrow \sigma_p(n_1) + \sigma_p(n_2) - \sigma_p(n_1 + n_2) = (A + B)(p - 1)$

$\Rightarrow \frac{\sigma_p(n_1)\sigma_p(n_2) - \sigma_p(n_1 + n_2}{p-1} = A + B =$ number of times we carry.

4 Question 4

4.1 Part a

$o_p(\binom{2n}{n}) = \frac{\sigma_p(D)+\sigma_p(n)-\sigma_p(2n)}{p-1}$ = Number of times we have to carry when adding $n+n$

As $p > \sqrt{2n} \Rightarrow p^2 > 2n$
$\Rightarrow 2n = a_0 + a_1 p$

Let $n = b_0 + b_1 p$
$\Rightarrow 2n = n + n = b_0 + b_1 p + b_0 + b_1 p = 2b_0 + 2b_1 p$

We claim we carry at most one time, but suppose we carry twice.
$\Rightarrow 2b_0 > p \Rightarrow 2b_0 = c_0 + p$
$2b_1 + 1 > p \Rightarrow 2b_1 + 1 = c_1 + p$
$\Rightarrow 2b_0 + 2b_1 p = c_0 + c_1 p + p^2 = a_0 + a_1 p + 0p^2$

As the expansion is unique, $\Rightarrow 1 = 0$, a contradiction.
$\Rightarrow$ We carry at most once.

$\therefore o_p(\binom{2n}{n}) \leq 1$

4.2 Part b

Suppose $p \geq 3 \Rightarrow 3p \leq p^2$
$\Rightarrow p^2 \geq 3p > 2n \Rightarrow p > \sqrt{2n}$
$\Rightarrow \sigma_p(\binom{2n}{n}) \leq 1$

Then $n = a_0 + a_1 p < \frac{3p}{2} \Rightarrow a_1 = 1, a_0 < \frac{p}{2}$ as
$a_1 = 2 \Rightarrow n \geq 2p > \frac{3p}{2} > n$

$\Rightarrow \sigma_p(n) = 1 + a_0 < 1 + \frac{p}{2}$

As $a_0 < \frac{p}{2}$, if $p \geq 3$, we do not carry in adding $n+n$
$\Rightarrow o_p(\binom{2n}{n} = 0 \Rightarrow p \nmid \binom{2n}{n}$

If $p = 2, \Rightarrow p \leq n < 3 \Rightarrow n = 2$
$\binom{2(2)}{2} = \binom{4}{2} = 6$

4.3 Part c

If $N \mid \binom{2n}{n} \Rightarrow m \leq o_p(\binom{2n}{n}$ = Number of carries from adding $n+n$
$\leq$ Number of digits in n
$\leq$ Number of digits in $2n$

$\Rightarrow 2n = a_0 + ... + a_m p^m + ... + a_k p^k, a_k \neq 0$
$\Rightarrow 2n \geq p^m = N$
$\Rightarrow m \leq \log_p(2n)$

5 Question 5

$$\binom{2n}{n} = \frac{(2n)!}{n!n!} = \frac{\prod_{k=1}^{n}(2k)\prod_{k=0}^{n-1}(2k+1)}{n!n!} \geq \frac{\prod_{k=1}^{n}(2k)\prod_{k=1}^{n-1}(2k)}{n!n!} \geq \frac{2^n(n!)(2^{n-1})(n-1)!}{n!(n)(n-1)!}$$

$$\geq \frac{2^{2n-1}}{n} \geq \frac{2^{2n}}{2n}$$

$$\Rightarrow \frac{2^{2n}}{2n} \leq \binom{2n}{n} \leq (2n)^{\sqrt{2n}-1}4^{\frac{2n}{3}}$$
$$2^{2n} \leq (2n)^{\sqrt{2n}}2^{\frac{4n}{3}}$$

$$\Rightarrow 2^{6n}4 \leq (2n)^{\sqrt{2n}}$$

$$\Rightarrow 2^{\frac{3n}{2}} \leq (2n)^{\sqrt{2n}}$$

$$\Rightarrow 2^{\frac{3n}{2}-\sqrt{2n}} \leq n^{\sqrt{2n}} = 2^{\log_2(n)\sqrt{2n}}$$

$$\Rightarrow \frac{3n}{2} - \sqrt{2n} \leq \log_2(n)\sqrt{2n}$$

$$\Rightarrow \frac{3}{2\sqrt{2}}\sqrt{n} \leq \frac{\ln(N)}{\ln(2)} + 1$$

which is clearly false for $n > 1000$, as $\sqrt{n}$ grows faster than $\ln N$