Elementary Number Theory
B. Math. (Hons.) First year
Instructor : B. Sury

Solutions to some problems from Chapter 1 of NZM
October 11, 2021

Ex. 30, section 1.2
If $(x, y) = g, xy = b$, then $b = xy = (x, y)[x, y] = g[x, y]$. As $g|[x, y]$, we have $g^2|b$.
Conversely, if $g^2h = b$, take $x = g, y = gh$.

Ex. 32, section 1.2
$n^k - 1 = (n - 1 + 1)^k - 1 = k(n - 1) + (n - 1)^2u$ for some integer u.
Therefore, $(n - 1)^2$ divides $n^k - 1$ if, and only if, $(n - 1)|k$.

Ex. 46, section 1.2
If $(a^n - b^n)|(a^n + b^n)$, then clearly $a \neq b$ and we may assume $(a, b) = 1$ because we may replace a and b by $a/(a, b)$ and $b/(a, b)$ respectively (we may get the smaller number to be 1 when we do this). Now $a^n - b^n$ divides $2a^n, 2b^n$ which implies it divides 2 as $(a^n, b^n) = 1$.
Therefore, $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}) = 1$ or 2. But the second factor is clearly $\geq a + b$ (as $n > 1$) which is ≥ 3 as $a > b \geq 1$. This is a contradiction of $(a - b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}) = 1$ or 2.

Ex. 47, section 1.2
Write $a = qb + r$ with $q \geq 0$ and $0 \leq r < b$. Then

$$2^a + 1 = 2^{qb+r} + 1 = 2^r(2^{qb} - 1) + 2^r + 1.$$

If $2^b - 1$ divides $2^a + 1$, then it divides $2^r + 1$; this implies $2^b - 1 \leq 2^r + 1 \leq 2^{b-1} + 1$. This is possible only when $b = 2$ whereas it is given that $a, b > 2$.

Ex. 51, section 1.2
Let q be any prime dividing $a+b$ and $\frac{a^p+b^p}{a+b} = \sum_{r=0}^{p-1} a^{p-1-r}(-b)^r$. Write $-b = qu + a$. Then,

$$\sum_{r=0}^{p-1} a^{p-1-r}(-b)^r = \sum_{r=0}^{p-1} a^{p-1-r}(qu + a)^r = qv + \sum_{r=0}^{p-1} a^{p-1} = qv + pa^{p-1}$$

for some integer v. As this is a multiple of q, it follows $q = p$ (otherwise, $q|a$ and hence $q|b$ which contradicts $(a, b) = 1$).
Now, we show that if p divides the GCD of $a + b$ and $\frac{a^p+b^p}{a+b}$, then p^2 does not divide this GCD. Indeed, similarly to the above argument, writing $-b = p^2t + a$, we have $\sum_{r=0}^{p-1} a^{p-1-r}(-b)^r == qv + \sum_{r=0}^{p-1} a^{p-1} =$

$p^2s + pa^{p-1}$ for some integer s. Thus, p^2 does not divide this because p does not divide a^{p-1}.

Ex. 53, section 1.2
$(n! + 1, (n + 1)! + 1) = (n! + 1, (n + 1)! - n!) = (n! + 1, n!n) = 1.$

Ex. 23, section 1.3
The given equations $ad - bc = \pm 1$, $u = am + bm, v = cm + dn$ imply clearly that the GCD of m and n divides both u and v. Now, the equations can also be rephrased in terms of matrices as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} u \\ v \end{pmatrix}$$

where the 2×2 matrix has determinant ± 1. Inverting the matrix above, we have

$$\begin{pmatrix} m \\ n \end{pmatrix} = \pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}.$$

In other words, $m = \pm(du - bv), n = \pm(-cu + av)$. Hence, the GCD of u and v divides both m and n.

Ex. 26, section 1.3
For $4n + 3$, $3, 11$ are the first two primes of this form, and consider the first $k \geq 2$ primes $p_1 < p_2 < \cdots < p_k$ of this form and consider $N = 4p_1p_2 \cdots p_k + 3$. All its prime factors cannot be of the form $4m + 1$ 9else, N itself would be of that form); hence there is a prime $p > 3$ of the form $4m + 3$ which divides N. Clearly, $p \neq p_1, \cdots, p_k$.
Similarly, for $6n + 5$, consider the first $r \geq 2$ primes $q_1, \cdots, q_r$ of this form and $M = 6q_1q_2 \cdots q_r + 5$ is divisible by at least one prime $q > 5$ of the form $6m + 5$ (else all prime factors will be of the form $6m + 1$ and so will M itself be). Then, $q \neq q_i$ for all $i \leq r$.

Ex. 27, section 1.3
If $n > 4$ is composite and p is the smallest prime dividing n, then $p \leq n/p$. If $p < n/p$, then both of them occur separately as factors in $(n-1)!$. Hence, $n|(n-1)!$. If $p = n/p$, then $n = p^2$. Note that p is odd as $n > 4$. But $2p$ also occurs as factor in $(n-1)! = (p^2 - 1)!$ since $2p \leq p^2 - 1$ as $(p-1)^2 \geq 2$. Therefore, again p^2 divides $(n-1)!$.

Ex. 40, section 1.3
If $N = (m + 1) + \cdots + (m + n) = \frac{n(2m+n+1)}{2}$ with $m \geq 0, n \geq 2$, then we will show N is not a power of 2. Indeed, if $N = 2^k$, then $2^{k+1} = n(2m + n + 1)$ which means both n and $2m + n + 1$ must be powers of 2. As $n > 1$, it must be even but then the number $2m+n+1$ is odd and cannot be a power of 2.

Conversely, if $N > 1$ is not of the form 2^k, then we will show it is expressible as sum of two or more consecutive positive integers. Now, there exists an odd prime dividing N and let p be the smallest such. If $N = p = 2k+1$ say, then $N = k + (k+1)$. If $N = pa$ with $a > 1$, then either $(p-1)/2 \leq a$ or $(p-1)/2 > a$ (the latter happens only if a is a power of 2 (otherwise, $a \geq p$ as it has an odd prime factor). In the first case, $k = (p-1)/2 \leq a$ and so,

$$pa = (2k+1)a = (a-k) + \cdots + (a-1) + a + (a+1) + \cdots + (a+k).$$

If $k = (p-1)/2 > a$; that is, $p > 2a+1$, then

$$ap = \left(\frac{p-2a+1}{2}\right) + \cdots + \left(\frac{p-1}{2}\right) + \left(\frac{p+1}{2}\right) + \cdots + \left(\frac{p+2a-1}{2}\right).$$

Ex. 48, section 1.3

$F_n = 2^{2^n} + 1$ implies $F_n - 2 = (2^{2^{n-1}})6 - 1 = (F_{n-1} - 1)^2 - 1 = F_{n-1}(F_{n-1} - 2)$.

In this manner, we obtain

$$F_n - 2 = F_{n-1}F_{n-2} \cdots F_1(F_1 - 2).$$

Therefore, F_n is coprime to all the F_m for $m < n$ (because a possible common factor dividing them divides 2 and must be 1 as the numbers are odd.

Ex. 19, section 1.4

I will leave it to students to work out a proof using generating functions, and here I give another proof.

We assume $n > 0$ and prove that $\sum_{k=0}^{n} \binom{m+1}{k}\binom{m+n-k}{m} = 0$. We will observe that the sum can be viewed as $(\Delta^{m+1}f)(0)$ for a polynomial of degree m (and hence, must be 0). In fact, consider $f(x) = \binom{x+n-1}{m}$. Then, $f(m+1-k) = \binom{m+n-k}{m}$. So,

$$0 = (\Delta^{m+1}f)(0) = \sum_{k=0}^{m+1}(-1)^k \binom{m+1}{k}\binom{m+n-k}{m}.$$

Note that the sum is actually from $k=0$ to n as $m+n-k \geq m$.

Ex. 21, section 1.4

Consider the polynomial $f(x) = \binom{x}{n}$. Then,

$$f'(x) = \lim_{h \to 0} \frac{\binom{x+h}{n} - \binom{x}{n}}{h}.$$

At $x = n$, we get $\sum_{k=1}^{n} \frac{1}{k}$.

On the other hand, $\binom{x+h}{n} = \sum_{k=0}^{n} \binom{h}{k}\binom{x}{n-k} = \binom{x}{n} + \sum_{k=1}^{n} \binom{h}{k}\binom{x}{n-k}$.

So, we have $\lim_{h\to 0} \frac{\binom{x+h}{n}-\binom{x}{n}}{h} = \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k}\binom{x}{n-k}$. Taking $x = n$, we get the asserted identity.