Number Thoery and Algebra Notes and Problems

Sava Spasojevic

July 15, 2019

The function

$$f : \mathbb{Z} \to \mathbb{Z}_5,\ a \mapsto [a]$$

is a homomorphism of additive groups.

$$f(a+b) = [a+b] = [a] + [b] = f(a) + f(b)$$

It is surjective, but it is not injective. This map is surjective since for $n \in \{0,1,2,3,4\}$, $b \equiv n \mod 5 \in \mathbb{Z}$. This map is not injective because

$$f(9) = f(29), 9 \neq 29$$

The function $f : G \times H \to G$ is a surjective homomorphism.

$$f((g,h)) = g$$

$$f((g,h) + (g',h')) = g + g' = f(gh) + f(g'h')$$

$$f(ghg'h') = f(gg'hh') = gg' = f(gh)f(g'h')$$

. If H is not the identity group then f is not one-to-one. Take $a \in H, a \neq e$.

$$f((e,e)) = f((e,a)), \text{but } (e,e) \neq (e,a)$$

Theorem: Let G, H be groups. If $f : G \to H$ is a hom, then

1. $f(e) = e$. This one is trivial.
2. $f(a^{-1})f(a) = e = f(a)^{-1}f(a)$

   $$f(a^{-1})f(a) = f(a)^{-1}f(a)$$

   Cancellation gives $f(a^{-1}) = f(a)^{-1}$
3. imf is a subgroup of H. $f(a), f(b) \in imf$. $f(a)f(b) = f(ab) \in imf$. $f(a)^{-1} \in imf$ for $f(a)$.
4. If f is injective, then $G \cong imf$. Say f injective. f is clearly surjective. done.

Cayleys Theorem: Every group G is isomorphic to a group of permutations.

Proof. Consider all the permutations of G, call it $p(G)$. $p(G)$ is too large to be isomorphic to G since if $|G| = n$, then $|p(G)| = n!$. Construct an injective homomorphism $f : G \to p(G)$. Then $G \cong imf \leq p(G)$. Fix $g \in G$. Define $\varphi_g : G \to G,\ l \mapsto gl$.

$$\varphi_g(w) = \varphi_g(m) \Rightarrow gw = gm \Rightarrow w = m$$

$$\text{Let } m \in G.\ f(g^{-1}m) = gg^{-1}m = m$$

This is a bijective map from G to G so $\varphi \in p(G)$. Define $f : G \to p(G), g \mapsto \varphi_g$. $m, w, l \in G$, $f(mw) = \varphi_{mw} = mwl = \varphi_m(\varphi_w(l)) = \varphi_m \circ \varphi_w = f(m) \circ f(w)$. f is a hom.

$$f(w) = f(m) \Rightarrow wl = ml \Rightarrow w = m$$

f is injective. Conclusion : $G \cong imf$. □

22. If $f : G \to H$ group iso, $T \leq G$, $T \cong f(T) := \{f(a) : a \in T\} \leq H$.

Proof. Consider $j : T \to f(T)$.

$$j(t) = j(r) \Rightarrow f(t) = f(r) \Rightarrow t = r$$

since f injective.

$$j(t) = f(t)$$

So, j is surjective.

$$j(tr) = f(tr) = f(t)f(r) = j(t)j(r)$$

. j is a hom. $T \cong f(T)$ □

21. If $G \cong H$ and $H \cong K$, then $G \cong K$.

$$f : G \to H,\ g : H \to K$$

$$g \circ f : G \to K$$

$g(f(w)) = g(f(m)) \Rightarrow g(w) = g(m) \Rightarrow w = m$. Injective. f is surjective as is g. Let $g(h) = k$. Let $f(m) = h$. Surjectivity follows.

$$g(f(wm)) = g(f(w)f(m)) = g(f(w))g(f(m))$$

Hom.

1. Compute the remainder when 37^{100} is divided by 29.

   soln:

$$\begin{aligned}
37 &\equiv 8 \mod 29 \\
37^2 &\equiv 1369 \mod 29 = 6 \\
37^4 = (37^2)^2 &\equiv 36 \mod 29 = 7 \\
37^8 = (37^4)^2 &\equiv 49 \mod 29 = 20 \\
37^{16} = (37^8)^2 &\equiv 400 \mod 29 = 23 \\
37^{32} = (37^{16})^2 &\equiv 529 \mod 29 = 7 \\
37^{64} = (37^{32})^2 &\equiv 49 \mod 29 = 20 \\
37^{100} = 37^{64} \cdot 37^{32} \cdot 37^4 = 20 \cdot 49 &\equiv 980 \mod 29 = 23
\end{aligned}$$

   The remainder is 23.

2. Compute the last two digits of 9^{1500}.

   soln: Perform a similar procedure starting at $9^3 = 729 \equiv 29 \mod 100$ and then squaring to obtain

$$9^{1500} = 9^{768} \cdot 9^{384} \cdot 9^{192} \cdot 9^{96} \cdot 9^{48} \cdot 9^2 = 7236395401 \equiv 1 \mod 100$$

   Therefore, the last two digits are 01.

3. Prove that for any integers a and b that $a^2 + b^2$ never leaves a remainder of 3 when divided by 4.

Proof. The squares of the elements in $\mathbb{Z}/4\mathbb{Z}$ are just 0 and 1. The sum of two squares is at most 2. Suppose

$$a^2 + b^2 = 4q + 3$$

Then

$$a^2 + b^2 \equiv 3 \mod 4$$

$$a^2 + b^2 = 3$$

which is a contradiction since in $\mathbb{Z}/4\mathbb{Z}$ the sum of two squares is at most 2. □

4. Prove that the square of any odd integer always leaves a remainder of 1 when divided by 8.

Proof. Let $k \in \mathbb{Z}$. $(2k+1)^2 = 4k^2+4k+1$. We show that $8 \mid 4k^2+4k$. First look at k^2+k. If k is even then $2 \mid k^2+k$. If k is odd, write $k = 2m+1, m \in \mathbb{Z}$. $k^2+k = 4m^2+6m+2$, which is even, hence divisible by 2. Thus, $2 \mid k^2+k$. Multiply by 4 to get $8 \mid 4k^2+4k$. So, odd integer $= (2k+1)^2 = 4k^2+4k+1 \equiv 1 \mod 8$. □

1.5) (Leibniz) If f and g are C^∞-functions, prove that

$$(fg)^{(n)} = \sum_{r=0}^{n} \binom{n}{r} f^{(r)} g^{(n-r)}$$

.

Proof. We proceed with mathematical induction on n. When $n = 1$, $(fg)^{(1)} = \binom{1}{0} f'g + \binom{1}{1} fg' = f'g + fg'$, which is the standard product rule. Suppose the statement is now true for n.

$$(fg)^{(n)} = \sum_{r=0}^{n} \binom{n}{r} f^{(r)} g^{(n-r)} = \binom{n}{0} fg^{(n)} + \binom{n}{1} f^{(1)} g^{(n-1)} + \binom{n}{2} f^{(2)} g^{(n-2)} + \ldots + \binom{n}{n} f^{(n)} g$$

$$\begin{aligned}
(fg)^{(n+1)} &= \binom{n}{0}[f^{(1)}g^{(n)} + fg^{(n+1)}] + \binom{n}{1}[f^{(2)}g^{(n-1)} + f^{(1)}g^{(n)}] + \binom{n}{2}[f^{(3)}g^{(n-2)} + f^{(2)}g^{(n-1)}] \\
&\quad + \ldots + \binom{n}{n-1}[f^{(n)}g^{(1)} + f^{(n-1)}g^{(2)}] + \binom{n}{n}[f^{(n+1)}g + f^{(n)}g^{(1)}] \\
&= \binom{n}{0} fg^{(n+1)} + \left[\binom{n}{0} + \binom{n}{1}\right] f^{(1)}g^{(n)} + \left[\binom{n}{1} + \binom{n}{2}\right] f^{(2)}g^{(n-1)} \\
&\quad + \ldots + \left[\binom{n}{n-1} + \binom{n}{n}\right] f^{(n)}g^{(1)} + \binom{n}{n} f^{(n+1)}g \\
&= \binom{n+1}{0} fg^{(n+1)} + \left[\binom{n}{0} + \binom{n}{1}\right] f^{(1)}g^{(n)} + \left[\binom{n}{1} + \binom{n}{2}\right] f^{(2)}g^{(n-1)} \\
&\quad + \ldots + \left[\binom{n}{n-1} + \binom{n}{n}\right] f^{(n)}g^{(1)} + \binom{n+1}{n+1} f^{(n+1)}g
\end{aligned}$$

Notice that a middle term of the sum, meaning that the exponents of f and g are not (0), is represented by

$$\left[\binom{n}{k} + \binom{n}{k+1}\right] f^{(k+1)} g^{(n-k)},\ 0 \le k \le n-1$$

Aside from notation, $f^{(k+1)}g^{(n-k)}$ obeys the same laws in the summation and the only term of interest is the coefficient

$$\begin{aligned}\binom{n}{k} + \binom{n}{k+1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k-1)!} \\ &= \frac{(k+1)n! + (n-k)n!}{k!(k+1)(n-k)(n-k-1)!} \\ &= \frac{(n+1)!}{(k+1)!(n-k)!} \\ &= \binom{n+1}{k+1}\end{aligned}$$

After adding all the binomial coefficients and simplifying, we get

$$\binom{n+1}{0} fg^{(n+1)} + \binom{n+1}{1} f^{(1)}g^{(n)} + \binom{n+1}{2} f^{(2)}g^{(n-1)} + \ldots + \binom{n+1}{n} f^{(n)}g^{(1)} + \binom{n+1}{n+1} f^{(n+1)}g$$

which equals

$$(fg)^{(n+1)} = \sum_{r=0}^{n+1} \binom{n+1}{r} f^{(r)}g^{(n+1-r)}$$

□

- Prove the Converse of Euclids Lemma.

Proof. Suppose that there is an integer $p \geq 2$ such that when p divides a product, it divides the factors of the product. If p is prime we're done. If p is not prime, then it is composite. Take this composite number to be in the form $[a, b]$ for some a, b. Then, $[a, b] \nmid a$ and $[a, b] \nmid b$, so no composite number can satisfy such a proposition. □

1.2) Let n be a composite integer. Show that there exists a prime p dividing n, with $p \leq n^{1/2}$.

Proof. Base case: $n = 4$. Pick $p = 2$. Then $2 \leq \sqrt{4} = 2$. This is true. Suppose that the statement holds for the first $n - 1$ composite integers. We show that this implies n. Since n composite, $n = ab$, with $1 < a < n$ and $1 < b < n$. If both are prime then take $p = \min(a, b)$. $n^{1/2} = (ab)^{1/2} \geq p$ since $ab \geq p^2$. WLOG suppose that a is composite. b can be either prime or composite, it won't change the result. By the induction hypothesis, $\exists p$ such that $p \mid a$ and $a \geq p^2$. So, $p \mid n$ and $n = ab \geq a \geq p^2$ or $n^{1/2} \geq p$. □

1.15) An integer a is called square-free if it is not divisible by the square of any integer greater than 1. Show that every positive integer n can be expressed uniquely as $n = ab^2$, where a and b are positive integers, and a is square-free.

Proof. The fundamental theorem of arithmetic says that $n = p_1^{e_1} \cdots p_r^{e_r}$ distinct primes. Take all p_i with odd exponent and move one of each out of the product. Then $n = p_k \cdots p_l(p_1^{e_1} \cdots p_r^{e_r})$. All the remaining $p_i's$ in the parenthesis now have even exponent. Factor out a 2 in each of the exponents and the remaining product in parenthesis is b. □

1.16) For each positive integer m, let I_m denote $\{0, \ldots, m-1\}$. Let a, b be positive integers, and consider the map

$$\tau : I_b \times I_a \to I_{ab},\ (s, t) \mapsto (as + bt) \mod ab$$

Show τ is a bijection if and only if $gcd(a, b) = 1$.

This is close to saying that if $gcd(n, m) = 1$, then $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$.

1.17) Let a, b, c be positive integers satisfying $\gcd(a, b) = 1$ and $c \geq (a-1)(b-1)$. Show that there exist non-negative integers s, t such that $c = as + bt$.

Proof. Since $\gcd(a,b)=1$ we have that $a\mathbb{Z}+b\mathbb{Z}=\mathbb{Z}$. Since $c\in\mathbb{Z},\ c\in a\mathbb{Z}+b\mathbb{Z}$. We use double induction to show that the inequality guarantees non-negative s and t. $S(1,1)$ is true since the minimal value for c is 0, with $s=0$ and $t=0$. Any greater value of c will assume greater positive values of s and t. Next $S(m,1)$ is true. $\gcd(m+1,1)=1$. This leads to $c\geq 0$. This means and s,t will be non-negative. Now, suppose $S(m,n)$ is true for all m. □

1.18) For each positive integer n, let D_n denote the set of positive divisors of n. Let n_1,n_2 be relatively prime, positive integers. Show that

$$f: D_{n_1}\times D_{n_2}\to D_{n_1n_2},\ (d_1,d_2)\mapsto d_1d_2$$

is bijective.

Proof. We prove injectivity via the contrapositive by saying that if $d_1\neq d_1'$ or $d_2\neq d_2'$ then $d_1d_2\neq d_1'd_2'$. Assume that $d_1\neq d_1'$. The prime factorization of d_1' contains at least one such $p_i^{e_i}$ where $\nu_{p_i}(d_1')>\nu_{p_i}(d_1)$. Let this number that is missing from d_1's factorization be called p for simplicity. The only way that $d_1d_2=d_1'd_2'$ is if the prime factorization of d_2 contains this p. But, this contradicts the fact that n_1 and n_2 are relatively prime since p is a factor that d_1' and d_2 both share, making it a common factor of n_1 and n_2 greater than 1. Let $d_1d_2\in D_{n_1n_2}$. Then pick $(d_1,d_2)\in D_{n_1}\times D_{n_2}$. We have that $f(d_1,d_2)=d_1d_2$. □

1.19) Let n be an integer. how that if $\{a_i\}_{i=1}^k$ is a pairwise relatively prime family of integers, where each a_i divides n, then their product $\prod_{i=1}^k a_i$ also divides n.

Proof. Pairwise relatively prime would mean that $gcd(a_1,\ldots,a_k)=1$. Since each a_i divides n and the a_i have no common factors, $\prod_{i=1}^k a_i \mid n$. □

1.21 Show that for all positive integers (including negatives would require a $\pm$ symbol, giving the abs val) a,b, we have:

1. $\gcd(a,b)\cdot\operatorname{lcm}(a,b)=|ab|$
2. $\gcd(a,b)=1\Rightarrow\operatorname{lcm}(a,b)=|ab|$.

Proof. Let $a,b\in\mathbb{Z}^+$.

1.
$$\begin{aligned}\gcd(a,b)\cdot\operatorname{lcm}(a,b)&=\prod_p p^{\min\{\nu_p(a),\nu_p(b)\}}p^{\max\{\nu_p(a),\nu_p(b)\}}\\&=\prod_p p^{\min\{\nu_p(a),\nu_p(b)\}+\max\{\nu_p(a),\nu_p(b)\}}\\&=\prod_p p^{\nu_p(a)+\nu_p(b)}\\&=ab\end{aligned}$$

2. Using the above, $\gcd(a,b)\cdot\operatorname{lcm}(a,b)=1\cdot\operatorname{lcm}(a,b)=\operatorname{lcm}(a,b)$.

□

1.26) HEY WHAT'S UP. Let n and k be positive integers, and suppose $x\in\mathbb{Q}$ such that $x^k=n$ for some $x\in\mathbb{Q}$. Show that $x\in\mathbb{Z}$.

Proof. Suppose that $x\notin\mathbb{Q}$. Then $\exists a\in\mathbb{Z}$ and $b\in\mathbb{N}: x=\frac{a}{b}$ with $\gcd(a,b)=1$. It follows that $a^k=nb^k$ or that $n\mid a^k$. Case 1: n is a power of a. Let $n=a^l$ for some $l\in[1,k]$. Then, $a^{k-l}=b\cdot b^{k-1}$ which implies that $b\mid a^{k-l}$, a contradiction. Case 2: n is a divisor of a. Let m be the integer such that $mn=a$. Then $ma^{k-1}=b^k$ or $m\mid b^k$, a contradiction. □

1.28) Show that for every positive integer k, there exist k consecutive composite integers. Thus, there are arbitrarily large gaps between primes.

Proof. This proof provides a new way of looking at $n!$. Consider $(k+1)!$. We can see that

$$\begin{aligned}
(k+1)!+2 &= [(k+1)(k)(k-1)\cdots(4)(3)+1]\cdot 2\\
(k+1)!+3 &= [(k+1)(k)(k-1)\cdots(4)(2)+1]\cdot 3\\
(k+1)!+4 &= [(k+1)(k)(k-1)\cdots(3)(2)+1]\cdot 4\\
&\vdots\\
(k+1)!+k &= [(k+1)(k-1)\cdots(3)(2)+1]\cdot k\\
(k+1)!+(k+1) &= [(k)(k-1)\cdots(3)(2)+1]\cdot (k+1)
\end{aligned}$$

so that $2 \mid (k+1)!+2,\ 3 \mid (k+1)!+3,\ \ldots,\ k+1 \mid (k+1)!+k+1$. This is a sequence of k composite consecutive integers. $n!$ provides all the integers needed to make this possible since it contains $n-1$ consecutive factors. □

1.31) Let n be a positive integer, and let 2^k be the highest power of 2 in the set $S := \{1,\ldots,n\}$. Show that 2^k does not divide any other element in S.

Proof. Suppose that is does divide another element in the set. This element has the form $s\cdot 2^k$ for some $s \geq 2$. So the element $2^k + \ldots + 2^k$ (added together s times) is in S. Since s takes it's minimum value at 2, $2^k + 2^k = 2^{k+1} \in S$. But, this contradicts the fact that k was the highest power of 2 in S. □

1.33) Let n be a positive integer, and let C_n denote the number of pairs of integers (a,b) with $a,b \in \{1,\ldots,n\}$ and $\gcd(a,b)=1$, and let F_n be the number of distinct rational numbers a/b, where $0 \leq a < b \leq n$.

1. Show that $F_n = (C_n+1)/2$.
2. Show that $C_n \geq n^2/4$.

Proof. Let $C = \{1,\ldots,n\}$ and F be the list of distinct rationals a/b where $0 \leq a < b \leq n$. Also, suppose that $C \to F$ is given by $(a,b) \mapsto a/b$ where any number in C that does not satisfy the given conditions on F is not included in F, but instead sent to some rational trash bin T.

1. We know that $\gcd(a,b) = \gcd(b,a)$. So, $1 \leq a < b \leq n$ forms a one-to-one map of pairs of elements in $C \setminus \{(1,1)\}$, namely $(a,b) \mapsto (b,a)$. This is because the pairs are distinct. We need only count (a,b) however, since (b,a) would form the rational number b/a violating the condition that the numerator is strictly less than the denominator. $(1,1)$ occurs only once in C. Thus, C_n is an odd number. We also neglect counting $(1,1)$ as a distinct rational number since $1<1$ fails. Counting, so far, gives $(C_n-1)/2$ terms. Included in F however, is the rational number $0/1$. So, $F_n = [(C_n-1)/2]+1 = (C_n+1)/2$, which is an integer since C_n+1 is even.

□

2.6) Let $a,b,n,n' \in \mathbb{Z}$ with $n>0, n'>0$, and $\gcd(n,n')=1$. Show that if $a \equiv b \mod n$ and $a \equiv b \mod n'$, then $a \equiv b \mod nn'$.

Proof. $a-b$ is a common multiple of both n and n'. Since n and n' are relatively prime, $\operatorname{lcm}(n,n') = nn'$. nn' must divide any common multiple of n and n', so $nn' \mid a-b$ or $a \equiv b \mod nn'$. □

2.9) Show that the equation $7y^3+2=z^3$ has no solutions $y,z \in \mathbb{Z}$.

Proof. Consider the equation $(7y^3 + 2 = z^3) \mod 7$. This is $z^3 \equiv 2 \mod 7$. In mod 7.

$$z^3 = 1, 8, 27, 48, 125, \text{or } 216$$

After 216 we cycle. We want to see if $z^3 - 2$ is ever divisble by 7. $7 \nmid -1, 7 \nmid 6, 7 \nmid 26, 7 \nmid 48, 7 \nmid 124, 7 \nmid 214$. So z^3 is never congruent to 2 in mod 7. Hence, the equation has no solutions. □

2.13) Let p be a prime, and let a, b, c, e be integers, such that $e > 0, a \not\equiv 0 \mod p^{e+1}$, and $0 \leq c < p^e$. Define N to be the number of integers $z \in L := \{0, \ldots, p^{2e} - 1\}$ such that

$$\eta(z) := \left\lfloor \frac{az + b \mod p^{2e}}{p^e} \right\rfloor = c$$

Show that $N = p^e$.

What the code is showing: Consider what would happen if $a \equiv 0 \mod p^{e+1}$, i.e. $a = kp^{e+1}$ for some $k \in \mathbb{Z}$. In η we can neglect the addition of b to az since all it does is shift the cycle of integers produced by $az \mod p^{2e}$. In other words, it does not affect the number of values for which z satisfies the given equality. We are left to consider the numbers produced by $kp^{e+1}z \mod p^{2e}$. This is the set of of multiples of $p^{e+1} \mod p^{2e}$, which, when divided by p^e and floored leaves only multiples of p. Thus, there are no solutions for values of c where $\gcd(c, kp) = 1$. This gives that $N < p^e$.

Proof. □

I used C++ to help understand how the truth value of the condition $a \not\equiv 0 \mod p^{e+1}$ changes the value of N. Let S_c be the set of z which solve the equation for a particular c. This code helps show that if the conditions of the problem are met, there is a bijection $\varphi : L \to \bigcup_{i=0}^{p^e} S_i$.

```cpp
#include <iostream>
#include <cmath>

using namespace std;

void testing(int p, int e, int a, int b);

//************************************************************
// WRITTEN BY SAVA SPASOJEVIC                                *
// testing(...) will give the varying values of              *
// z that satisfy the equation given in the problem.         *
// It can be easily seen that if a \equiv 0 mod p^{e+1}      *
// a cycle of length p^e is not permitted and therefore not  *
// all values of c will be captured.                         *
//************************************************************

int main()
{
    int p1 = 2;
    int e = 2;

    cout << "Test 1" << endl;
    cout << "------" << endl;

    int a = 3, b = 7;

    testing(p1, e, a, b);

    return 0;
}
```

```
31
32 void testing(int p, int e, int a, int b)
33 {
34    int pe = static_cast<int>(pow(p,e)), p2e = static_cast<int>(pow(p, 2*e));
35    cout << "value of a = " << a << endl;
36    cout << "value of b = " << b << endl;
37    cout << "value of e = " << e << endl;
38    cout << "value of p = " << p << endl;
39    cout << "value of p^e = " << pe << endl;
40    cout << "value of p^e*p = " << pe*p << endl;
41    cout << "Check pe*p | a: ";
42    if (pe*p % a != 0)
43       cout << "false\n";
44    else
45       cout << "true\n";
46    cout << "value of p^2e = " << p2e << endl;
47
48    int L[2401]; cout << "L = { ";
49    for (int i = 0; i < p2e; i++)
50    {
51       L[i] = i;
52       cout << L[i] << " ";
53    }
54    cout << "}" << endl;
55    int S[122], s_index = 0, f_index = 0;
56    int V = 0;
57    double eqtn = 0;
58
59    for (int j = 0; j < pe; j++) //pe different values of c \in {0,...,pe-1}
60    {
61       cout << endl;
62       cout << "c = " << j << endl;
63       cout << "_____" << endl;
64       for (int i = 0; i < p2e; i++)
65       {
66          eqtn = (((a * L[i]) + b) % p2e) / pe;
67          V = floor(eqtn);
68          cout << "f( [" << a << "*" << L[i] << " + " << b << " mod " << p2e << "↩
               ]/" << pe << " ) = "
69             << "f( " << ((a * L[i]) + b) % p2e << "/" << pe << " ) = " << V;
70          if (V == j)
71          {
72             S[f_index] = L[i];
73             f_index++;
74             cout << " <- MATCH";
75          }
76          cout << endl;
77       }
78       cout << "List of MATCH(z) values: { ";
79       for (int i = s_index; i < f_index; i++)
80          cout << S[i] << " ";
81       cout << "}" << endl;
82       s_index = f_index;
83    }
84 }
```

2.14) Find an integer a such that $a \equiv 1 \bmod 3, a \equiv -1 \bmod 5,$ and $a \equiv 5 \bmod 7$.

Proof. We use the proof of the Chinese Remainder Theorem to construct integers

$$e_i \equiv \begin{cases} 1 \bmod n_i, & i = j \\ 0 \bmod n_j, & i \neq j \end{cases}$$

where $n_1 = 3, n_2 = 5, n_3 = 7$, so that $a \equiv \sum_{i=0}^{3} e_i a_i \equiv a_j \bmod n_j$.

$$\begin{aligned}
\prod_{i=1}^{3} n_i &= 3 \cdot 5 \cdot 7 = 105 \\
n_1^* &= 105/3 = 35 \\
n_2^* &= 105/5 = 21 \\
n_3^* &= 105/7 = 15 \\
t_1 &\equiv n_1^* \bmod n \Rightarrow t_1 = 140, \text{ so } e_1 = t_1 n_1^* = 4900 \\
t_2 &\equiv n_2^* \bmod n \Rightarrow t_2 = 126, \text{ so } e_2 = t_2 n_2^* = 2646 \\
t_3 &\equiv n_3^* \bmod n \Rightarrow t_3 = 120, \text{ so } e_3 = t_3 n_3^* = 1800 \\
\sum_{i=0}^{3} e_i a_i &= 11254
\end{aligned}$$

Another solution is $a' \equiv 11254 \bmod 105 = 19$. Thus, we can take $a = 19$ and the equations work out. □

2.15) If you want to show that you are a real nerd, here is an age guessing game you might play at a party. You ask a fellow party-goer to divide his age by each of the numbers 3, 4, and 5, and tell you the remainders. Show how to use this information to determine his age.

Proof. Accurately guess the persons decade, i.e. are they in their 20s, 30s, 40s? This will speed up the process. Compute the values of $e_i = t_i n_i^*$ and you'll find that they are 40, 45, and 36. Obtain the remainders a_i from the person. Compute $40a_1 + 45a_2 + 36a_3$ and subtract 60 until you are at a reasonable age. However, if you guess the decade correctly, you only need to find the ones digit of the sum. That way you skip the process of subtracting 60 or even computing the entire sum, and are left with adding this digit to their decade. □

2.19) Use induction. The property holds for all m when $\alpha \in \mathbb{Z}_n^*$ since for $m > 0$, α^{-m} exists as multiplicative inverses exist in $\mathbb{Z}_n^*$. Do induction again.

2.20) Let p be an odd prime. Show that $\sum_{\beta \in \mathbb{Z}_p^*} \beta^{-1} = \sum_{\beta \in \mathbb{Z}_p^*} \beta = 0$.

Proof. We know that $\mathbb{Z}_p^*$ is closed and inverses are uniquely determined so that the set of inverses in $\mathbb{Z}_p^*$ is equal to the set of elements in $\mathbb{Z}_p^*$. We obtain that $\sum_{\beta \in \mathbb{Z}_p^*} \beta^{-1} = \sum_{\beta \in \mathbb{Z}_p^*} \beta$. Notice that $\sum_{\beta \in \mathbb{Z}_p^*} \beta = p(p+1)/2$. $(p+1)/2$ is an integer since p was said to be odd. When modding by p we see that the sum is equivalent to 0. □

2.21) Let p be an odd prime. Show that the numerator of $\sum_{i=1}^{p-1} 1/i$ is divisible by p.

Proof.

$$\begin{aligned}
\sum_{i=1}^{p-1} 1/i &= 1 + \frac{1}{2} + \ldots + \frac{1}{p-1} \\
&= \frac{p_1 + \ldots + p_{p-1}}{(p-1)!}
\end{aligned}$$

Where $p_i = \frac{(p-1)!}{i}$. The numerator is a sum of $p-1$ distinct integers. If we mod the sum by p we will get the sum of $p-1$ distinct elements in $\mathbb{Z}_p^*$, which is just $\mathbb{Z}_p^*$. By the proof of 2.20, such a sum was said to be divisible by p. Hence, the numerator is divisible by p. □