31 Rigorous Proofing Examples

Ahmed Metwally

July, 2022

The arithmetic are based on laws that build up the general and more advanced theories. They can be expressed as follows.

1. *Closure Property*
$$a + b \in \mathbb{Z}$$
$$a - b \in \mathbb{Z}$$

2. *Commutative property*
$$a + b = b + a$$
$$a \times b = b \times a$$

3. *Identity Property*
$$a + 0 = a$$
$$a \times 1 = a$$

4. *Associative property*
$$a + (b + c) = (a + b) + c$$
$$a \times (b \times c) = (a \times b) \times c$$
$$a \times b \in \mathbb{Z}$$

5. *Distributive Property*
$$a \times (b + c) = a \times b + a \times c$$

6. *Well ordering Principle* Every nonempty subset S of the positive integers has a least element.

7. *Cancellation law*: If a, b, and c are integers with $a \times c = b \times c$, $c \neq 0$, then $a = b$.

8. There is a unique element $0 \in \mathbb{Z}$ such that $\forall a \in \mathbb{Z}, 0 + a = a + 0 = a$

9. *additive inverse:* $\forall a \in \mathbb{Z}$, there is a unique element $-a \in \mathbb{Z}$ such that $a + (-a) = (-a) + a = 0$

10. *Trichotomy*: If $a \in \mathbb{Z}$, then is has one of the following three states
$$a = 0,$$
$$a > 0,$$
$$a < 0$$

I am going to mention these axioms along this rigrous proofing article to build your rigorous understanding of math. You may think of that any number multiplied by zero is zero for granted, but it is actually can be proven using the previous axioms.

1 Reasoning

P1: $d|a,\ d|b \Rightarrow d|(ar+bs)$. True in $\mathbb{Z}$.
Proof: We have $d|a \Rightarrow a = kd$, where $k \in \mathbb{Z}$ from (D3). By multiplying the first equation by r, where $r \in \mathbb{Z}$, and the second equation be s where $s \in \mathbb{Z}$. $(A7I)$

$$ra = r(kd), \qquad \text{(A7I), (A1)} \qquad \text{(1a)}$$
$$ra = (rk)d, \qquad \text{(A1)} \qquad \text{(1b)}$$
$$sb = s(md), \qquad \text{(A7I), (A1)} \qquad \text{(1c)}$$
$$sb = (sm)d, \qquad \text{(A1)} \qquad \text{(1d)}$$

By adding(A7I) the two equations: (1b) and (1d):

$$ra + sb = (rk)d + (sm)d, \qquad \text{(A1)} \qquad \text{(2a)}$$
$$ra + sb = d(rk + sm), \qquad \text{(A3)} \qquad \text{(2b)}$$
$$d|(ra + sb), \qquad \text{(A3),(D3)} \qquad \text{(2c)}$$
$$d|(ar + bs), \qquad \text{(A2)} \qquad \text{(2d)}$$

$rk + sm \in \mathbb{Z}$ because of the closure property in $\mathbb{Z}$.

P2: $0 \times a = 0\ \forall a$. True in $\mathbb{Z}$.
Proof:

$$0 \times a = (0+0) \times a, \qquad \text{(A4)} \qquad \text{(3a)}$$
$$0 \times a = 0 \times a + 0 \times a, \qquad \text{(A3)} \qquad \text{(3b)}$$
$$0 \times a + (-0 \times a) = (0 \times a + 0 \times a) + (-0 \times a), \qquad \text{(A6)} \qquad \text{(3c)}$$
$$(0 \times a + (-0 \times a)) = 0 \times a + (0 \times a + (-0 \times a)), \qquad \text{(A1)} \qquad \text{(3d)}$$
$$0 = 0 \times a + 0, \qquad \text{(A6),} \qquad \text{(3e)}$$
$$0 = 0 \times a \qquad \text{(A4)} \qquad \text{(3f)}$$

P3: $a < b$ and $b < c \Rightarrow a < c$.
Proof:
We have if $a < b \Rightarrow b = a + k$, and $b < c \Rightarrow c = b + m$ for some $k, m \in \mathbb{N}$ from (D5).
By substituting,

$$c = (a + k) + m, \qquad \text{(A1)} \qquad \text{(4a)}$$
$$c = a + (k + m), \qquad \text{(A1)} \qquad \text{(4b)}$$
$$c > a, \qquad \text{(D5)} \qquad \text{(4c)}$$
$$a < c, \qquad \text{(D7)} \qquad \text{(4d)}$$

P4: $a < b$ and $c > 0 \Rightarrow ac < bc$. True in $\mathbb{Z}$.
Proof:
We have if $a < b \Rightarrow b = a + k$, for some $k \in \mathbb{N}$ from (D5).
By multiplying both sides by c,

$$bc = (a + k)c, \qquad \text{(closure property)} \qquad (5a)$$
$$bc = (ac) + (kc), \qquad \text{(A3)} \qquad (5b)$$
$$bc = ac + (kc), \qquad \text{(A1)} \qquad (5c)$$
$$bc > acc, \qquad \text{(D5)} \qquad (5d)$$

Since we have k and $c \in \mathbb{N}$, $(kc) \in \mathbb{N}$ by (A7I).

P5: There are no integers strictly between 0 and 1.
Proof:
Suppose to the contrary that the set $S = \{x : 0 < x < 1, x \in \mathbb{Z}\}$ contain all integers between 0 and 1. So, by WOP S has a least element, call a.

$$0 < a < 1$$

By multiplying all elements by a(A7I), we get

$$0 \times a < a^2 < a \times 1, \qquad \text{(P4)} \qquad (6a)$$
$$0 \times a < a^2 < a, \qquad \text{(A5)} \qquad (6b)$$
$$0 < a^2 < a, \qquad \text{(P2)} \qquad (6c)$$
$$0 < a^2 < a < 1, \qquad \text{(P3)} \qquad (6d)$$

$0 \times a < a^2 < a \times 1 \Rightarrow 0 < a^2 < a < 1$. However, this contradicts the minimality of a since we have supposed that a is the least element in the set S.

P6: If m, n are positive integers and $m|n$ then $m < n$.
Proof:
$m|n \Rightarrow n = km$ for some $k \in \mathbb{N}$. Suppose there exists a set $S = \{x|x = \frac{n}{m}\} \cup \mathbb{N}$. This set is non-empty because $n = \frac{n}{1}$
By WOP, there exists a least element, call $a \in \mathbb{N}$ where $a > 1$ because if $a = 1$ then $m = n$. So, we have $n = a \times m$

$$a = a + 1 - 1 \qquad (7a)$$
$$n = (a + 1 - 1)m, \qquad \text{(A6)} \qquad (7b)$$
$$n = ((a - 1) + (+1))m, \qquad \text{(A1)} \qquad (7c)$$
$$n = (a - 1)m + 1 * m, \qquad \text{(A3)} \qquad (7d)$$
$$n = (a - 1)m + m, \qquad \text{(A5)} \qquad (7e)$$
$$\text{Since} (a - 1)m \in \mathbb{N}, m > n, \qquad \text{(D5)} \qquad (7f)$$

P7: Every non-empty subset of Z which is bounded above has a largest element.

Proof:

Suppose to the contrary that the set S is bounded above but doesn't have a largest element. So, by definition of bounded above, there exists $Q+1 \notin S$. So, $S = \{x | x < Q+1\} \cap \mathbb{Z}$. So, $Q \in S$. Since there isn't a largest element, there exists an element k such that $Q < k < Q+1$. From (A6), we can add $(-Q)$ to all terms, so $Q + (-Q) < k + (-Q) < Q + 1 + (-Q)$.

$$Q < k < Q + 1 \tag{8a}$$
$$Q + (-Q) < k + (-Q) < Q + 1 + (-Q), \quad \text{(A6)} \tag{8b}$$
$$(Q + -Q) < k + (-Q) < 1 + (Q - Q), \quad \text{(A1)} \tag{8c}$$
$$(0) < k + (-Q) < 1 + (0), \quad \text{(A6)} \tag{8d}$$
$$0 < k + (-Q) < 1, \quad \text{(A4)} \tag{8e}$$

From (P2), there is no integer between 0 and 1$\Rightarrow\Leftarrow$. So, Q is a largest element.

P8: If $m \neq 0$ and $a = b$(mod m) then the common divisors of a, m are the same as those of b, m. True in $\mathbb{Z}$.

Proof:

We have $a = b$(mod m) $\Rightarrow m|(a-b)$(D3) $\Rightarrow a - b = mk$(Dr4) where $k \in \mathbb{Z}$(D3). Suppose that $d = gcd(b, m)$. Because $d|m$ and $d|b$, there exists integers e, q such that $b = ed$ and $m = qd$. By substituting, we get:

$$a - b = (mk) \tag{9a}$$
$$a - b + b = mk + b, \quad \text{(A5)} \tag{9b}$$
$$a + (-b + b) = km + b, \quad \text{(A1)} \tag{9c}$$
$$a + 0 = km + b, \quad \text{(A5)} \tag{9d}$$
$$a = km + b, \quad \text{(A4)} \tag{9e}$$
$$a = k(qd) + (ed), \quad \text{(substituting)} \tag{9f}$$
$$a = (kq)d + (e)d, \quad \text{(A1)} \tag{9g}$$
$$a = d(kq + e), \quad \text{(A3)} \tag{9h}$$
$$d|a \quad \text{(D3)} \tag{9i}$$

By symmetry, we get $(a, m)|b \& (a, m)|a$ and $(b, m)|a \& (b, m)|b$. So, we must have $(a, m) = (b, m) = (a, b)$ from the definition of *gcd*.

P9: Every integer greater than 1 has a prime factor.
Proof:
Suppose to the contrary that the set S contains all elements with no prime factors. $S = \{m | p \not| m, \text{where } p \text{ is a prime}\} \cap \mathbb{N}$.
By WOP, there exists a least element call, a. If a is a prime, then from (D20) $a = a \times 1$. So, $a|a$. So, $a \notin S$. If not, then there exists $1 < b, c < a$ such that $b \times c = a$. $1 < b, c < a$ because if $b, c > a, \Rightarrow b \times c > a$, which will not be equal to a. Because $a > 1$ and a isn't a prime, there exists from (D20) $b \times c = a$ where $1 < b, c < a$. Since a is the least element in the set S. So, b, c have a prime divisor. So, there exists p such that $p_1|c$. But $p_1|c$ and $c|a$. From lemma 1, $p_1|a$.

---

2 Lemmas:

Lemma1: If $a|b$ and $b|c$, then $a|c$.
Proof:
From (D3), $a|b \Rightarrow b = ka$ and $b|c \Rightarrow c = mb$, where $k, m \in \mathbb{Z}$.
By substituting,

$$c = m(ka), \tag{10a}$$
$$c = (mk)a, \qquad \text{(A1)} \tag{10b}$$
$$a|c \qquad \text{(D3)} \tag{10c}$$

Lemma2 If $a = A_1 + a_2 i$ and $b = b_1 + b_2 i$, then $N(a) * N(b) = N(ab)$
Proof:

$$N(a) \times N(b) = (a_1^2 + a_2^2) \times (b_1^2 + b_2^2), \tag{11a}$$
$$= (a_1 b_1)^2 + (a_1 b_2)^2 + (a_2 b_1)^2 + (a_2 b_2)^2 \tag{11b}$$
$$ab = (a_1 b_1 - a_2 b_2) + (a_1 b_2 + a_2 b_2) i \tag{11c}$$
$$N(ab) = (a_1 b_1 - a_2 b_2)^2 + (a_1 b_2 + a_2 b_2)^2 \tag{11d}$$
$$= (a_1 b_1)^2 + (a_1 b_2)^2 + (a_2 b_1)^2 + (a_2 b_2)^2 \tag{11e}$$
$$= N(a) \times N(b) \tag{11f}$$

Lemma3 a, b, we have one of these three cases: $a > b$, $b > a$, or $a = b$.
Proof: From trichometry, we have $(a-b) = k \in \mathbb{N}$ or $(b-a) = k \in \mathbb{N}$ or $a - b = 0$.

$$
\begin{aligned}
(a-b) &= k, && \text{A7II} && (12a)\\
(a-b)+(b) &= k+(b), && \text{A6} && (12b)\\
a+(-b+b) &= k+(b), && \text{A1} && (12c)\\
a+(0) &= k+(b), && \text{A6} && (12d)\\
a &= k+(b), && \text{A4} && (12e)\\
a &> b && \text{D5} && (12f)
\end{aligned}
$$

Second case,

$$
\begin{aligned}
(b-a) &= k, && \text{A7II} && (13a)\\
(b-a)+(a) &= k+(a), && \text{A6} && (13b)\\
b+(-a+a) &= k+(a), && \text{A1} && (13c)\\
b+(0) &= k+(a), && \text{A6} && (13d)\\
b &= k+(a), && \text{A4} && (13e)\\
b &> a && \text{D5} && (13f)
\end{aligned}
$$

Third case,

$$
\begin{aligned}
(a-b) &= 0, && \text{A7II} && (14a)\\
(a-b)+(b) &= 0+(b), && \text{A6} && (14b)\\
a+(-b+b) &= 0+(b), && \text{A1} && (14c)\\
a+(0) &= (b), && \text{A6, A4} && (14d)\\
a &= (b), && \text{A4} && (14e)\\
a &= b && \text{D5} && (14f)
\end{aligned}
$$

3 Prove or Disprove and Salvage if possible

P10: $a, b \in \mathbb{N} \Rightarrow$ there exist $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.
Proof:
From **Lemma3**, we have either $a > b$ or $b > a$ or $a = b$. If $a = kb$, then $q = k$ and $r = 0$. If $a < b$, then $q = 0$ and $r = a < b$.
If $a > b$, Suppose that S is a set such $S = \{a - bx | \forall x \in \mathbb{Z}\} \cap \mathbb{N}$. This set is nonempty because for $q = 0$, $a - b * 0 = a \in \mathbb{N}$ by (A4). Now, we have showed that the set S is nonempty, so we can apply the WOP. Suppose that $r = a - bq$ is the least element in this set. Let's assume for the sake of contradiction that $r \geq b$. We will have $a-bq \geq b \Rightarrow a-bq-b \geq 0 \Rightarrow a-b(q+1) \geq 0$. However, $a-b(q+1) < r$ but this contradicts the minimality of r. So, $0 \leq r < b$.

P11: $a, b \in \mathbb{N} \Rightarrow$ the Diophantine equation $ax + by = 1$ has an integral solution (x, y).
Proof:
False, counter example, there is no (x, y) such that $2x + 4y = 1$.
Salvage: It is true of $gcd(a, b) = 1$
Let $S = \{n \in \mathbb{Z} | n > 0, n = ax + by, \text{for some } x, y \in \mathbb{Z}\}$. S is nonempty because if $(x, y) = (a, b)$, then $a^2 + b^2 > 0$. By WOP, there exists a least element of S, call m.
If $m > 1$, the $m|a$ and $m|b$ can't be true simultaneously because $(a, b) = 1$.
WLOG, let $m \nmid a$, so by division algorithm(P10), there exists $q, r \in \mathbb{Z}$ such that $a = mq+r$ where $0 < r < m$. Suppose (x_0, y_0) is a solution.

$$
\begin{aligned}
r &= a - mq, && \text{A6} && (15a)\\
&= a - (ax_0 + by_0)q, && \text{substitution} && (15b)\\
&= a - (ax_0q + by_0q), && \text{substitution} && (15c)\\
&= a(1 - x_0q) + b(-y_0q), && \text{A3} && (15d)
\end{aligned}
$$

This is a contradiction since it contradicts the minimality of m. So, $m = 1$ has a solution.

P12: $a|bc$ and $a \nmid b \Rightarrow a|c$. True in $\mathbb{Z}$.
Proof:
We have $a|bc \Rightarrow bc = ka$ where $k \in \mathbb{Z}$ (D3). If $a \nmid b \Rightarrow b = qa + r$ where $q \in \mathbb{Z}$ and $0 \leq r < a$. By multiplying both sides by by c, we get

$$
\begin{aligned}
b(c) &= (qa + r)c, && \text{A7I} && (16a)\\
bc &= qac + rc, && \text{A3} && (16b)\\
ka &= c(qa + r), && \text{A3} && (16c)\\
a|c & && \text{D3} && (16d)
\end{aligned}
$$

P13: $x \in \mathbb{Z}_p \Rightarrow x^p = x$ in $\mathbb{Z}$. Here p is a positive prime.
Proof: We have $x, 2x.3x, ..., (p-1)x \equiv 1, 2, 3, ..., (p-1) \pmod{p}$. This is because we are just walking in circle of mods p, so by multiplying a constant by every number it will span through the whole modular circle since $(x, p) = 1$. So, by multiplying all of these terms, we would have

$$
\begin{aligned}
x^{p-1} \times (p-1)! &\equiv (p-1)! (\text{mod} p)\\
x^{p-1} &\equiv 1 (\text{mod } p)\\
x^p &\equiv x (\text{mod } p)
\end{aligned}
$$

P14: If $u \in U_m$ has order n and $(k, n) = 1$ then u^k has order n.
Proof: Suppose to the contrary that there exists a number less than n, which is the order of u^k, call l. We have $(u^k)^l \equiv 1 \Rightarrow u^{kl} \equiv 1$. So, $n|kl$, but $(k, n) = 1$. By FTA, $n|l$, but we supposed that $l < n \Rightarrow\Leftarrow$. So, the least number that is divided by n is n itself. So, n is the order of u^k.

P15: If $a|n$ and $b|n \Rightarrow (ab)|n$. True in $\mathbb{Z}$.
Proof: *False* $4|8$ and $8|8$, but $32 \not| 8$.
Salvage: it works when $(a, b) = 1$. if $a|n$, $b|n \Rightarrow n = ak$, $n = mb$ for some values of $k, m \in \mathbb{Z}$.
Since $(a, b) = 1 \Rightarrow a = qb + r$, where $0 < r < b$ from (P10).

$$ax + by = 1, \qquad \text{P11} \qquad (17a)$$
$$n((ax) + (by)) = 1 * n, \qquad \text{A7I} \qquad (17b)$$
$$n(ax) + n(by) = n, \qquad \text{A3, 5} \qquad (17c)$$
$$(bm)(ax) + (ak)(by) = n, \qquad \text{Substituting} \qquad (17d)$$
$$(ba)(mx) + (ba)(ky) = n, \qquad \text{A1} \qquad (17e)$$
$$(ba)(mx + ky) = n, \qquad \text{A3} \qquad (17f)$$
$$(ab)(mx + ky) = n \qquad \text{A2} \qquad (17g)$$
$$ab|n \qquad \text{D3} \qquad (17h)$$

P16: π is a prime in $\mathbb{Z}$[i] $\iff$ $N(\pi)$ is a prime in $\mathbb{Z}$.
False because, 3 is a prime in $\mathbb{Z}[i]$, but $N(3) = 9$ which isn't a prime.
Salvage: If $N(\pi)$ is a prime in $\mathbb{Z}$ with $p \equiv 3 (\text{mod } 4)$, then π is a prime in $\mathbb{Z}[i]$.
Proof:
Suppose that $\pi = p$ be a prime with 3(mod 4) isn't a prime in $\mathbb{Z}[i]$ Then, $\pi = (a_1 + a_2 i)(b_1 + b_2 i)$. $N(\pi) = (a_1^2 + a_2^2)(b_1^2 + b_2^2) = p^2$. The nontrivial factorization for this equation is

$$a_1^2 + a_2^2 = p$$

$$b_1^2 + b_2^2 = p$$

Since $p \equiv 3 (\text{mod } 4)$, it can't be expressed as a sum of two squares. This is because we can't express any square as 3(mod 4) or 2(mod 4). So, the sum of the any two squares won't be a 3(mod 4).

P17: If a, n, m are natural numbers then $(a^n-1, a^m-1) = a^{(n,m)}-1$.
Proof:

$$a^m \equiv 1(\text{mod } gcd(a^n-1, a^m-1)) \tag{18a}$$
$$a^n \equiv 1(\text{mod } gcd(a^n-1, a^m-1)) \tag{18b}$$
$$a^{mx} \equiv 1(\text{mod } gcd(a^n-1, a^m-1)) \tag{18c}$$
$$a^{ny} \equiv 1(\text{mod } gcd(a^n-1, a^m-1)) \tag{18d}$$
$$a^{mx+ny} \equiv 1(\text{mod } gcd(a^n-1, a^m-1)) \tag{18e}$$
$$a^{gcd(n,m)} \equiv 1(\text{mod } gcd(a^n-1, a^m-1)) \tag{18f}$$
$$a^{gcd(n,m)} - 1 | gcd(a^n-1, a^m-1) \tag{18g}$$
$$a^{gcd(n,m)} - 1 = gcd(a^n-1, a^m-1) \tag{18h}$$

P18: If $u_i \in U_m$ has order $n_i (i = 1, 2)$ and if $(n_1, n_2) = 1$ then $u_1 \times u_2$ has order $n_1 \times n_2$.
Proof: Suppose that the order of $(u_1 \times u_2)$ is l. So, $(u_1 \times u_2)^l \equiv 1(\text{mod } m)$

$$(u_1 \times u_2)^{ln_1} \equiv 1^{n_1}(\text{mod } m) \tag{19a}$$
$$(u_1)^{ln_1} \times (u_2)^{ln_1} \equiv 1(\text{mod } m) \tag{19b}$$
$$\text{So, } (u_2)^{ln_1} \equiv 1(\text{mod } m) \tag{19c}$$

This implies that $n_2 | ln_1$. Similarly, $n_1 | ln_2$. Since the $gcd(n_1, n_2) = 1$, the minimum value of l that can satisfy both equations is $(n_1 \times n_2)$.

---

4 Numerical problems:

P19: Obtain the required resuts without changing to base ten. (a)$(434)_5 \times (242)_5 = (?)_5$; (b)$(5352)_7 - (626)_7 = (?)_7$; (c)$(21432)_5 \div (34)_5 = (?)_5$; (d)$(5631)_7 = (?)_5$.
Answer:
(a)$(434)_5 \times (242)_5 = (233233)_5$
(b)$(5352)_7 - (626)_7 = (4423)_7$
(c)$(21432)_5 \div (34)_5 = (303.\overline{230343320})$
(d)$(5631)_7 = (31111)_5$

P20: Calculate the following elements in $\mathbb{Z}_{29}$: -1, -7, $\frac{1}{2}$, $\frac{1}{7}$, $\frac{8}{3}$, $\sqrt{6}$, $\sqrt{-7}$.
Answer:
(a)$-1 \equiv 28 + 29k$ (mod 29), where $k \in \mathbb{Z}$.
(b)$-7 \equiv 22 + 29k$ (mod 29), where $k \in \mathbb{Z}$.
(c)$(\frac{1}{2}) \equiv 15 + 29k$ (mod 29), where $k \in \mathbb{Z}$.
(d)$\frac{1}{7} \equiv 25 + 29k$ (mod 29), where $k \in \mathbb{Z}$.
(e)$\frac{8}{3} \equiv 22 + 29k$ (mod 29), where $k \in \mathbb{Z}$.
(f)$\sqrt{6} \equiv 6 + 29k$ (mod 29), where $k \in \mathbb{Z}$.
(g)$\sqrt{-7} \equiv 14 + 29k$ (mod 29), where $k \in \mathbb{Z}$.

P21: Make a table of "logarithms" for $\mathbb{Z}_{17}$. Use it to find all solutions in $\mathbb{Z}_{17}$ of (a) $7x = 6$, (b) $5x^2 = 7$, (c) $x^4 = 1$.
Answer:
Table of "logarithms" after taking 3 as a generator.

$log_3 a$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
a	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

(a)

$$7x = 6$$
$$log_3 7x = log_3 6 (\text{mod } 16)$$
$$log_3 7 + log_3 x = log_3 6 (\text{mod } 16)$$
$$11 + log_3 x = 15 (\text{mod } 16)$$
$$log_3 x = 4 (\text{mod } 16)$$
$$x = 13$$

(b)

$$5x^2 = 7$$
$$log_3 5x^2 = log_3 7 (\text{mod } 16)$$
$$log_3 5 + 2log_3 x = log_3 7 (\text{mod } 16)$$
$$5 + 2log_3 x = 11 (\text{mod } 16)$$
$$log_3 x = 3 (\text{mod } 8)$$
$$x = 10, 7$$

(c)

$$x^4 = 1$$
$$log_3 x^4 = log_3 1 (\text{mod } 16)$$
$$4log_3 x = log_3 1 (\text{mod } 16)$$
$$4log_3 x = 16 (\text{mod } 16)$$
$$log_3 x = 4 (\text{mod } 4)$$
$$x = 13, 1, 4, 16$$

P22: Find an x in $\mathbb{Z}_{249}$ such that $119x + 5 \equiv 0$ in $\mathbb{Z}_{249}$.
Answer: Using Euclidean algorithm:

$$249 = 119 * 2 + 11$$
$$119 = 11 * 10 + 9$$
$$11 = 9 * 1 + 2$$
$$9 = 2 * 4 + 1$$
$$2 = 1 * 2 + 0$$

Using linear combination method: we get a solution for $249x + 119y = 1$ $(x, y) = (-54, 113)$. So,$x \equiv 5 * 113 (\text{mod } 249)$. $x \equiv 67 (\text{mod } 249)$

P23: Find the continued fraction of $\sqrt{18}$ and find the first convergent which approximates $\sqrt{18}$ within $\frac{1}{4000}$. Explain.
Answer:
The integral part of $\sqrt{18}$ is 4.

$$4+\frac{1}{\frac{1}{\sqrt{18}-4}}=4+\frac{1}{4+\frac{1}{\frac{1}{4-(\frac{\sqrt{18}+4}{2})}}}=4+\frac{1}{4+\frac{1}{8+\frac{1}{4+\frac{1}{8+\frac{1}{\cdots}}}}}$$

So, we conclude that $\sqrt{18}=[4;\overline{4,8}]$

P24: Calculate $\mu(7007)$, $\tau(7007)$, $\sigma(7007)$, and $\phi(7007)$.
Answer: $7007=7^2*13*11$ - $\mu(7007)=0$ because there is 7^2 in its factorization.
-$\tau(7007)=3*2*2=12$
-$\sigma(7007)=9576$
-$\phi(7007)=\phi(7^2)*\phi(13)*\phi(11)=6*7*12*10=5040$

P25: Use the table in P21 to find all the generators in U_{17}. Find all the prefect squares in U_{17}. Justify.
Answer:
- We have if g is a generator, g^m is a generator iff $(m,|U_17|)=1$. So, when $log_3 a=1,3,5,7,9,11,13,15$, a is a generator. All generators in U_17 are 3, 10, 5, 11, 14, 7, 12, and 6.
- Prefect squares are 9, 13, 15, 16, 8, 4, 2, 1.

P26: Is $5+2i$ a unit in $(\mathbb{Z}[i])_{3+7i}$? Explain.
Answer:
No, because $5+2i|3+7i$.

$$\frac{3+7i}{5+2i}\times\frac{5-2i}{5-2i}=\frac{29+29i}{29}=1+i$$

,
So, we can't find a number that can be multiplied by $5-2i$ to give us 1.

P27: Find all integers x which satisfy the following two congruence simultaneously: $x=13(\text{mod }101)$ and $x=17(\text{mod }103)$.
Answer:
Using Chinese remainder theorem, $x\equiv 10214\ (\text{mod }10403)$

P28: Find all solutions of the equation $x^2 = 14$ in $\mathbb{Z}_{143}$.
Answer:
By using the quadratic formula:

$$\frac{\pm\sqrt{56}}{2} \equiv \pm 72\sqrt{56} (\text{mod } 143)$$

By solving again for $\sqrt{56}$, we get:

$$\frac{\pm\sqrt{56 * 4}}{2} \equiv \pm 72\sqrt{81} \equiv \pm \times 72 \times 9 \equiv \pm 76 \equiv 76, 67 (\text{mod } 143)$$

$$\pm 72 \times 76 \equiv \pm 38 \equiv 38, 105 \equiv (\text{mod } 143)$$

$$\pm 72 \times 67 \equiv \pm 27 \equiv 27, 116 \equiv (\text{mod } 143)$$

---

5 Miscellaneous Problems

P29: p prime $> 2 \Rightarrow \{(\frac{p-1}{2})!^2\} = (-1)^{(\frac{p+1}{2})} (\text{mod p})$. For which p does this show that -1 is a square in $\mathbb{Z}_p$?
Proof: We have

$$(p-1) \equiv -1 (\text{mod } p)$$

$$(p-2) \equiv -2 (\text{mod } p)$$

$$...$$

$$\frac{(p+1)}{2} = -\frac{(p-1)}{2} (\text{mod } p)$$

So, by multiplying all terms with each other, we get:

$$(p-1)! = (-1)^{(\frac{p-1}{2})} \times (\frac{(p-1)}{2})!^2 (\text{mod } p)$$

From Wilson's theorem, we get:

$$-1 = (-1)^{(\frac{p-1}{2})} \times (\frac{(p-1)}{2})!^2 (\text{mod } p)$$

$$(-1)^{(\frac{p+1}{2})} = (\frac{(p-1)}{2})!^2 (\text{mod } p)$$

P30: Let p be a rational prime and let k be a natural number. Then

$$\sum_{a=1}^{p-1} a^k = 0$$

In $\mathbb{Z}_p$ unless $k \equiv 0 (\text{mod } p-1)$ in which case the sum is -1 in $\mathbb{Z}_p$
Proof: We have $a = 1, 2, .., p-2, p-1$. When raising these mods to a power it will yield the same mods since we are dealing with modular circle and $(p, a) = 1$. So, $a^k = 1, 2, .., p-2, p-1$. By adding all of these mod, we will get 0 because every number has its inverse such that their sum will be p. So, this whole sum will be a multiple of p which is 0 in $\mathbb{Z}_p$.
When $k \equiv 0 (\text{mod } p-1)$, by fermat's last theorem, $a^{(p-1)} - 1 \equiv$ (mod p). So, in this case the sum will add up to -1 instead of 1.

P31: $n \in \mathbb{N} \Rightarrow$

$$\sum_{d|n, d>0} \phi(d) = n$$

Proof: Consider this list

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \frac{4}{n}, \frac{5}{n} ... \frac{n}{n}$$

Since there are n numbers in the list, we may represent it as a quotient of relatively prime integers by reducing each number in the original list to its lowest terms. The numbers in the new list will have n's divisor as their common denominator. Exact $\phi(d)$ of the numbers will have d as their denominator if d divides n. (this is the meaning of lowest term). As a result, the new list contains (summation of $\phi(d)$). We get the intended outcome since both lists include the same number of terms.