HW 4 Discrete

Bayard Walsh

October 2022

1 Number Theory

a) If p is prime, and a is any integer not divisible by p, then $a^{p-1} \equiv_p 1$

By theorem 10.2, For any prime p ,$\varphi(p) = p - 1$. Therefore, $a^{p-1} \equiv_p 1$ equals $a^{\varphi(p)} \equiv_p 1$
As p is prime, and a is any integer not divisible by p, then $p > 1$ and p and a are co-prime. By Euler's Theorem, $a^{\varphi(p)} \equiv_p 1$. As $a^{p-1} \equiv_p 1$ equals $a^{\varphi(p)} \equiv_p 1$, $a^{p-1} \equiv_p 1$
Therefore, $a^{p-1} \equiv_p 1$

b) If p is prime, and a is any integer not divisible by p, then $a^?$ is an inverse of a modulo p.
Let $? = p - 2$, so a^{p-2} is an inverse of a modulo p
Consider $a * a^{p-2}$. This simplifies to a^{p-2+1} or a^{p-1}
By 1)a, $a^{p-1} \equiv_p 1$, meaning that $a * a^{p-2} \equiv_p 1$, or a^{p-2} is an inverse of a modulo p

c) Calculate 7^{66} mod 15 by hand.
By Corollary 10.6, as 7 and 15 are co-prime, $15 > 1$, and $66 \geq 0$, $7^{66} \equiv_{15} 7^{66 mod \varphi(15)}$
By Theorem 10.3, consider 5,3, as distinct primes.
Therefore, as $\varphi(15) = \varphi(5 * 3)$, $\varphi(15) = (5 - 1)(3 - 1)$
Therefore, $\varphi(15) = 8$
Consider $7^{66 mod 8}$ mod 15
(66 mod 8) $= 2$ as $8 * 8 = 64$
Therefore $7^{66 mod 8} \equiv_{15} 7^2$
Therefore, $49 \equiv_{15} 4$
Therefore 7^{66} mod 15 equals 4

d) Calculate $3^{3^{103}}$ mod 11 by hand.
As 3 and 11 are co-prime, by Corollary 10.6, $3^{3^{103}} \equiv_{11} 3^{3^{103} mod \varphi 11}$
Consider $3^{103} mod \varphi 11$. As 11 is prime, $\varphi 11 = 11 - 1$, or 10
Consider 3^{103} mod 10. By Corollary 10.6, as 3 and 10 are co-prime, 3^{103} mod

10 equals $3^{103 mod \varphi 10}$ mod 10
Consider $103 mod \varphi 10$. By Theorem 10.3, consider 5,2, as distinct primes.
Therefore, as $\varphi 10 = \varphi(5 * 2)$, $\varphi 10 = (5-1)(2-1)$, or 4
Therefore $103 mod \varphi 10$ equals $103 mod 4$, which mods down to 3.
Therefore, we have 3^{103} mod 10 equals 3^3 mod 10. 27 mod 10 is 7.
Therefore, $3^{3^{103}}$ mod 11 equals 3^7 mod 11.
$27 * 27 * 3$ mod 11 equals $6 * 6 * 3$ mod 11, by modding down. $36 * 3$ mod 11 equals $3 * 3$ mod 11, or 9.
Therefore $3^{3^{103}}$ mod 11 is 9.

e)
If $N = 35$, $E = 5$, $C = 11$, and assume that N and M are relatively prime
Consider $\varphi(35)$.Consider 7,5, as distinct primes and factors of 35. By Theorem 10.3, $\varphi(35) = (7-1)(5-1)$, or 28
Let D be some integer, such that D is the inverse of E modulo $\varphi(35)$.
Consider $ED \equiv_{\varphi(35)} 1$, by definition of inverse
Substitution for E and $\varphi(35)$, so that $5D \equiv_{24} 1$
Therefore $24|(5D-1)$, meaning that $D = 5$
Using the Decryption formula, $M = (C^D \bmod N)$
Substitution, $M = (11^5 \bmod 35)$
Therefore, $M = (121 * 121 * 11 \bmod 35)$
Therefore, $M = (16 * 16 * 11 \bmod 35)$, by modding down multiplication rule
Therefore, $M = (16 * 176 \bmod 35)$
Therefore, $M = (16 * 1 \bmod 35)$
Therefore, $M = 16$

2 Induction

a)**For all positive integers N there exists some integer M where $M^2 \leq N < (M+1)^2$.**
Proof by induction:
Statement: Let there be a positive integer N such that there exists some integer M where $M^2 \leq N < (M+1)^2$.
Base case:
$N = 0$, $0^2 \leq 0 < (0+1)^2$
$M = 0$ is a solution. Therefore, true.
Inductive hypothesis: $M^2 \leq N < (M+1)^2$
Let K be an integer, such that $K^2 \leq N+1 < (K+1)^2$
Let $K = M$. As $M^2 \leq N$, $K^2 \leq N+1$.
Also, as $N < (M+1)^2$, $N+1 \leq (K+1)^2$
Therefore, we have $K^2 \leq N+1 \leq (K+1)^2$ for some integer K
Consider case where $N+1 < (K+1)^2$. This holds for inductive hypothesis, so we are done.
Consider case where $N+1 = (k+1)^2$. Let $k = m+1$. As we know $N < (M+1)^2$, we have $N+1 < (M+2)^2$

Therefore, For all positive integers N there exists some integer M where $M^2 \leq N < (M+1)^2$.

b)**For the statement, Let there be a positive integer N such that there exists some integer M where $M^2 \leq N < (M+1)^2$, prove that M is unique**

First, assume that there exists a k such that k is less than m.

Therefore, $k^2 \leq N < (k+1)^2$

Smallest possible k element is $k = M-1$, which means that $(M-1)^2 \leq N < M^2$, which contradicts $M^2 \leq N$

Second, assume that there exists a k such that k is greater than m.

Therefore, $k^2 \leq N < (k+1)^2$

Greatest possible k element is $k = M+1$, which means that $(M+1)^2 \leq N < (M+2)^2$, which contradicts $N < (M+1)^2$

As M cannot be a greater or smaller element, M is unique.

c)**Prove $\sum_{i=1}^{n}(-1)^i * i^2 = (-1)^n * (n(n+1))/2$**

Statement: $\sum_{i=1}^{n}(-1)^i * i^2 = (-1)^n * (n(n+1))/2$ holds for all positive integers n

Base case: $n = 1$

$(-1)^1 * (1(1+1))/2$

This reduces to $-1 * 2/2$, or -1, which equals $\sum_{i=1}^{1}(-1)^1 * 1^2$

Therefore, the base is true

Inductive step:

Consider $\sum_{i=1}^{k+1}(-1)^i * i^2$

Therefore, $(\sum_{i=1}^{k}(-1)^i * i^2) + ((-1)^{k+1} * (k+1)^2)$

By inductive hypothesis, $((-1)^k * (k(k+1))/2) + ((-1)^{k+1} * (k+1)^2)$

Rewrite $(-1)^k * (k(k+1))/2$ as $-1((-1)^k * (k(k+1))/)2$, or $(-1)^{k+1} * -(k(k+1))/2$

Therefore, $(-1)^{k+1}((k+1)^2 - (k(k+1))/2)$

Expand to $(-1)^{k+1}(k^2 + 2k + 1 - (k(k+1))/2)$

Which is $(-1)^{k+1}((2k^2 + 4k + 2 - k^2 - k)/2)$

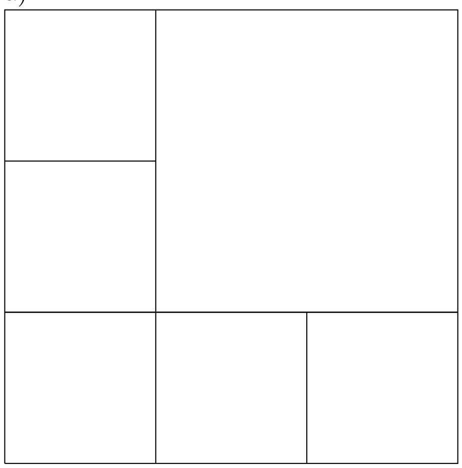
This simplifies to $(-1)^{k+1}((k^2 + 3k + 2)/2)$

Rewrite as $(-1)^{k+1}((k+1)(k+2)/2)$

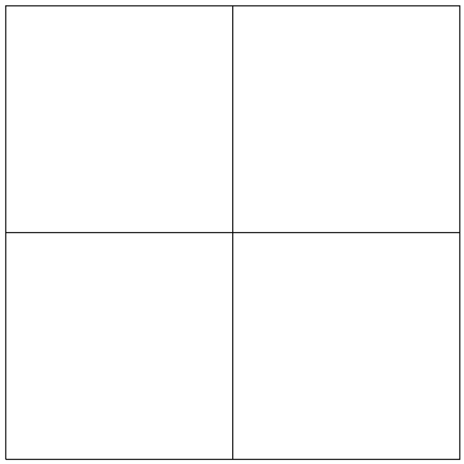
Thus we have shown that $\sum_{i=1}^{n}(-1)^i * i^2 = (-1)^n * (n(n+1))/2$ holds for $n = k+1$. Therefore $\sum_{i=1}^{n}(-1)^i * i^2 = (-1)^n * (n(n+1))/2$ holds for all $n \in \mathbf{N}$

3 Squaring Up

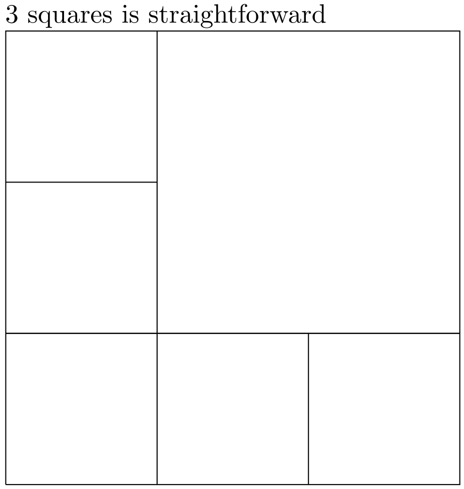
a)



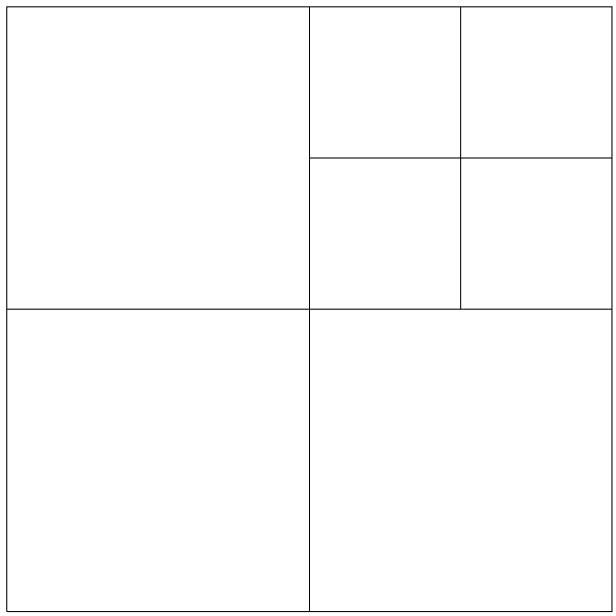
b)
20 squares. Currently 17 squares, - 1 (square to be divided up) + 4 (added amount of squares)
c)
Prove that for all $n > 5$,there exist integers $a \in \{6, 7, 8\}$ and $m \leq 0$ such that $n = a + 3m$.
Strong Induction Proof:
Base case: $n = 6, 7, 8, 9$
$6 = 6 + 3 * 0$
$7 = 7 + 3 * 0$
$8 = 8 + 3 * 0$
$9 = 6 + 3 * 1$
Inductive case: Let $k \in \mathbf{N}$ be arbitrary with $k \geq 9$ and assume for all $6 \leq j \leq k$ that $j = a + 3m$ for some $a, b \in \mathbf{N}$. Consider $n = k + 1$ Since $k \geq 9$, we have that $k - 3 \geq 6$ and $k - 3 = a + 3m$ with $a, b \in \mathbf{N}$. Then $k + 1 = a + 3(m + 1)$.
d)
Prove that for any $n > 5$, a square can be divided into n smaller non-overlapping squares.
Strong Induction Proof: Base case: $n = 6, 7, 8$
Consider the following squares:



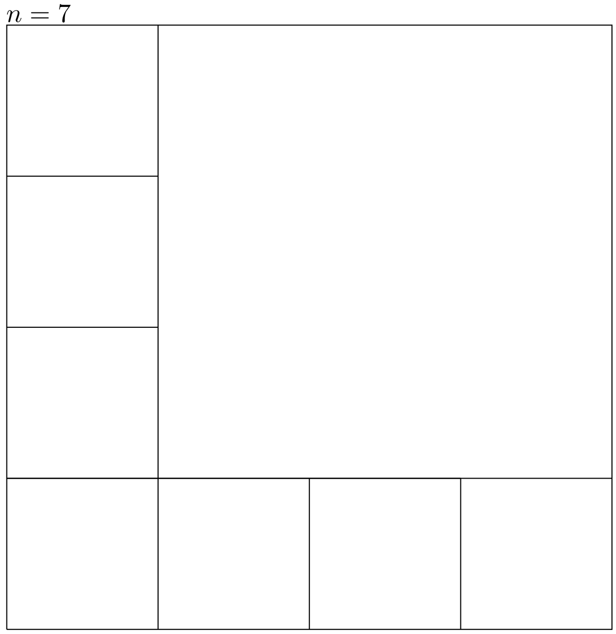
$n = 4$ While this is not in the base case, it indicates that given a square, adding 3 squares is straightforward



$n = 6$



$n = 7$



$n = 8$

Therefore, propose the formula $n = a + 3m$, where $a \in \{6, 7, 8\}$. As shown by $n = 4$, any square can be divided into 4 smaller squares (or adding increments of 3 to an amount of already non-overlapping squares will be always cause there to be n non-overlapping squares), hence $a + 3m$, where a is the base set and $3m$ is amount of squares one can add

By 4)c, For all $n > 5$,there exist integers $a \in \{6, 7, 8\}$ and $m \geq 0$ such that $n = a + 3m$.
Therefore, for any $n > 5$, a square can be divided into n smaller non-overlapping squares.

4 Irreducibility

a)
The following set is T-irreducible, from the set of $\{1, 2, ..., 20\}$
The set of $\{4, 7, 10, 13, 19\}$
This set is all intersections between $\{1, 2, ..., 20\}$ and T-set, excluding values with a factor other than itself in the set. In this case, that only removes 16, as 4 is also a factor, so 16 is not T-irreducible

b) Prove that for all $a, b \in T$ and $c \in N$, if $a = bc$, then $c \in T$.
By definition of set T all numbers in the set can be reduced to $3K + 1$. Therefore, $[a]_3 = 1$ and $[b]_3 = 1$
As, $a = bc$, consider $[a]_3 = [bc]_3$
By modding down, $[1]_3 = [c]_3$
By modular rules, $[c]_3 = 1$.
Therefore, for some positive integer K, $c = 3K + 1$, so $c \in T$

c) Prove that every element of T greater than 1 can be written as a product of T-irreducible integers.

Base case: Smallest element of T greater than 1 is 4. 4 is T-irreducible, therefore, it is T-irreducible with itself.
Statement: Let N be an element of T, and assume that there is some integer k such that $k < N, k \in T$ and $k > 1$. Assume that k can be written as the product of smaller T-irreducible factors.
Inductive Hypothesis:
Consider if N is prime or if N is T-irreducible. Therefore, $Div(N) \cap T$ will always be $\{1, N\}$. Therefore, if N is prime or T-irreducible, it's T-irreducible with itself, and proof is complete.
Assume it isn't. By definition of an element of T which is not T-irreducible, $Div(N)$ has one or more factors in common with T. Let c be integer such that $c|N$, and a be an integer such that $ca = N$. By 4b), because $c \in T$ and $N \in T$, then $a \in T$. Therefore, if $Div(N)$ has one or more factors in common with T it can be written as smaller T-irreducible factors, which meets the induction hypothesis.
Therefore, every element of T greater than 1 can be written as a product of T-irreducible integers

d) Prove, via a counterexample, that factorization into T -irreducible integers is not unique up to reordering.
100 is a counterexample.
$10 * 10$ is a factorization of 100. As Div(10)=$\{1, 2, 5, 10\}$, and $Div(10) \cap T = \{1, 10\}$, it is T -irreducible
$4 * 25$ is also a factorization of 100. As $Div(4) = \{1, 2, 4\}$, and $Div(4) \cap T = \{1, 4\}$, it is T -irreducible. As $Div(25) = \{1, 5, 25\}$, and $Div(25) \cap T = \{1, 25\}$, it is also T-irreducible.
Therefore, 100 has can be factorized into T-irreducible integers in 2 ways which aren't unique to up reordering. Therefore, factorization into T -irreducible integers is not unique up to reordering.

5 Collaborators List

Hunter Smith, Grey Sign, Nafis Khan