Worksheet 1

Andre Ye[1]

[1]University of Washington, MATH 402

+Draft date October 8, 2023.

Problem 1

If r, s, t are positive integers, how many positive divisors does $2^r 3^s 5^t$ have?

Let a and b be integers with $b \neq 0$. b is a divisor of a if $b|a$, or equivalently, $a = bc$ for some integer c. Any divisor of $2^r 3^s 5^t$ must have the form $2^a 3^b 5^c$, where $0 \leq a < r$, $0 \leq b < s$ and $0 \leq c < t$. We will prove this by reductio. Suppose d cannot be expressed in the form $2^a 3^b 5^c$. We claim d is a divisor of $2^r 3^s 5^t$. Let us express d as $2^a 3^b 5^c \cdot q$, where $2 \nmid q$, $3 \nmid q$, $5 \nmid q$, and $q > 1$. Every integer d which cannot be expressed as $2^a 3^b 5^c$ can be expressed as such due to the Fundamental Theorem of Arithmetic. Since d is a divisor of $2^r 3^s 5^t$, there exists an integer k such that $dk = 2^r 3^s 5^t \implies k \cdot 2^a 3^b 5^c \cdot q = 2^r 3^s 5^t$. Dividing both sides by $2^a 3^b 5^c$ yields $kq = 2^{r-a} 3^{s-b} 5^{t-c}$. The truth of this statement is equivalent to the truth of the statement $q | 2^{r-a} 3^{s-b} 5^{t-c}$. Theorem 1.4 states that if $a|bc$ and $(a,b) = 1$, then $a|c$. Consider $q|(2)(2^{r-a-1} 3^{s-b} 5^{t-c})$. We know that $(q,2) = 1$ because the theoretically maximum possible value of (a,b) is $\min(a,b)$, or 2 in this case, but we know $2 \nmid q$. By Theorem 1.4, this means that $q|2^{r-a-1} 3^{s-b} 5^{t-c}$. We can rewrite this as $q|(2)(2^{r-a-2} 3^{s-b} 5^{t-c})$. Using the same reasoning as above, from Theorem 1.4. and $(q,2) = 1$, it must be true that $q|2^{r-a-2} 3^{s-b} 5^{t-c}$. We can repeat this process, exploiting Theorem 1.4. and the fact that $(q,2) = 1$, $(q,3) = 1$, and $(q,5) = 1$ to continuously eliminate factors, until we end up finally at $q|5$. There are four numbers which divide 5: ± 1 and ± 5. Since $q > 1$, $q \notin \{-1, 1\}$. Since $5 \nmid q$, $q \notin \{-5, 5\}$. This is a contradiction. Therefore, d must be expressible in the form $2^a 3^b 5^c$ to be a divisor of $2^r 3^s 5^t$. $\square$

Given this, we simply need to select all the possible combinations of values of a, b, c. This yields $(r+1)(s+1)(t+1)$ possibilities (the $+1$ to include the zeroth exponent). From the "uniqueness" guarantee of the Fundamental Theorem of Arithmetic, there is no possibility of double-counting because the base of each exponent is a prime number.

Problem 2

If p is prime and p is divide by 10, show that the remainder is one of $1, 3, 7, 9$.

Strictly speaking, this statement is false, as 2 is a prime number but its remainder when divide by 10 is 2. However, we will show the statement holds for $p > 2$ using a proof by contradiction. Suppose that there exists some prime p such that the remainder when dividing by 10 is *not* in $\{1, 3, 7, 9\}$. By the division algorithm, this means that the remainder will be one of $\{0, 2, 4, 5, 6, 8\}$. In the case that the remainder is in the set $\{0, 2, 4, 6, 8\}$, p can be rewritten as $10k + 2r$ for some integers r, k. For instance, if the remainder is 0, $r = 0$; if the remainder is 2, $r = 1$; if the remainder is 4, $r = 2$, and so on. Then, p can be rewritten as $2(5k + r)$, which means that $2|p$. However, by the definition of a prime number, the only numbers which divide p are ± 1 and $\pm p$. For all $p \neq 2$, this is a contradiction. In the case that the remainder is 5, p can be rewritten as $10k + 5$ for some integer k. Then, p can be rewritten as $5(2k + 1)$, which means $5|p$. For all $p \neq 5$, this is a contradiction. Therefore, it must be the case that the remainder of a prime number p when divided by 10 is either 1, 3, 7, or 9. $\square$

Problem 3

What is $[8^{2023}] \in \mathbb{Z}_9$*?*

We can rewrite $[8^{2023}]$ as a product of congruence classes: $[8] \otimes [8] \otimes ... \otimes [8] = [8]^{2023}$. From Theorem 2.3., $[a] = [c]$ iff $a \equiv_n c$. We know that $8 \equiv_9 -1$; therefore, $[8] = [-1]$. As such, we can rewrite $[8]^{2023}$ as $[-1]^{2023}$, or alternatively as $[(-1)^{2023}]$. $(-1)^{2023} = -1$, as $(-1)^k = 1$ if $2|k$ and -1 if not. Therefore, $[8^{2023}] = [-1]$. By Theorem 2.3. again, $[-1] = [8]$. As such, $[8^{2023}]$ in $\mathbb{Z}_9$ is $[8]$.

Problem 4

If $a \in \mathbb{Z}$*, prove that* a^2 *is not congruent to 2 modulo 4 and or 3 modulo 4.*

Per the division algorithm/theorem, every integer a can be written as $4n + r$, where $n, r \in \mathbb{Z}$, $0 \leq r < 4$. a^2 is $16n^2 + 8nr + r^2$. There are four values r can take on: 0, 1, 2, 3. If $r = 0$, the expression simplifies to $16n^2$, which is 0 modulo 4 because it can be rewritten as $4(4n^2) + 0$. If $r = 1$, the expression simplifies to

$16n^2+8+1$, which is 1 modulo 4 because it can be rewritten as $4(4n^2+2)+1$. If $r=2$, the expression simplifies to $16n^2+16n+4$, which is 0 modulo 4 because it can be rewritten as $4(4n^2+4n+1)$. Lastly, if $r=3$, the expression simplifies to $16n^2+24n+9$, which is 1 modulo 4 because it can be rewritten as $4(4n^2+6n+2)+1$. Therefore, the square of an integer will always be either 0 or 1 modulo 4. $\square$

Problem 5

Prove that for any classes $[a],[b] \in \mathbb{Z}_n$, $[a] \oplus [b] = [b] \oplus [a]$.

We know that $[a] \oplus [b] = [a+b]$. Addition between integers is commutative (i.e. $a+b=b+a$), so therefore $[a+b]=[b+a]$. We can rewrite $[b+a]$ as $[b] \oplus [a]$. Since this is a direct chain of equivalences, we have that $[a] \oplus [b] = [b] \oplus [a]$. $\square$

Problem 6

Find an element $[a]$ in $\mathbb{Z}_7$ such that every nonzero element of $\mathbb{Z}_7$ is a power of $[a]$.

There are six nonzero elements of $\mathbb{Z}_7$: $[1],[2],[3],[4],[5],[6]$. Let $[a]=[3]$. Then we have $[a]^2=[2]$. This is because $[a]^2=[3]^2=[3^2]=[9]$ and $9 \equiv_7 2$. Likewise, $[a]^3=[6]$, $[a]^4=[4]$, $[a]^5=[5]$, $[a]^6=[1]$. Therefore, we have expressed every nonzero element of $\mathbb{Z}_7$ as a power of $[3]$.