| | | |
|---|---|---|
| **Name:** | **GSI:** | **DISC #:** |

# Solutions to Homework 5.

**Prob 1.** Find a formula for $\sum_{k=0}^{m} \lfloor \sqrt[3]{k} \rfloor$.

**Solution:** First note that any sum $\sum_{k=0}^{m} f(k)$ where $f(k)$ is a function from $\mathbb{Z}_+$ to $\mathbb{Z}_+$ is in fact the total number of (integer) points of the type $(k, h)$ where the first coordinate corresponds to our summation index $k$ and the second coordinate (denoted $h$ for "height") corresponds to the positive integer heights that do not exceed the value $f(k)$. In other words, it is the total number of points in the set

$$S = \cup_{k=0}^{m} \cup_{h \in \mathbb{N}} \{(k,h) : h \leq f(k)\} = \cup_{h \in \mathbb{N}} \cup_{k=0}^{m} \{(k,h) : f(k) > h-1\}.$$

That is, $\sum_{k=0}^{m} f(k) = |S|$. Notice next that the set $S$ is a disjoint union, over all possible natural values $h$, of its subsets $S_h = \{(k,h) : f(k) > h-1\}$, $h \in \mathbb{N}$. Thus

$$\sum_{k=0}^{m} f(k) = |S| = \sum_{h \in \mathbb{N}} |S_h|. \tag{1}$$

Now apply this reasoning to the function $f(k) = \lfloor \sqrt[3]{m} \rfloor - \lfloor \sqrt[3]{k} \rfloor$. We see that $f(k) > 0$ for the following values of $k$: $k = 0, \ldots, \lfloor \sqrt[3]{m} \rfloor^3 - 1$, which gives us $|S_1| = \lfloor \sqrt[3]{m} \rfloor^3$. Further, $f(k) > 1$ for $k = 0, \ldots, (\lfloor \sqrt[3]{m} \rfloor - 1)^3 - 1$, which gives $|S_2| = (\lfloor \sqrt[3]{m} \rfloor - 1)^3$, and so forth. The last nonempty set is $S_{\lfloor \sqrt[3]{m} \rfloor}$ of size $|S_{\lfloor \sqrt[3]{m} \rfloor}| = 1$ corresponds to the only value $k = 0$ that works for it. So, the formula (1) implies

$$\sum_{k=0}^{m} f(k) = |S| = \sum_{h \in \mathbb{N}} |S_h| = \sum_{j=1}^{\lfloor \sqrt[3]{m} \rfloor} j^3.$$

By the well-known formula for the sum of cubes (see the book), this gives us

$$\sum_{k=0}^{m} f(k) = \frac{\lfloor \sqrt[3]{m} \rfloor^2 (\lfloor \sqrt[3]{m} \rfloor + 1)^2}{4}.$$

Now we must transition from the designed sum $\sum_{k=0}^{m} f(k) = \sum_{k=0}^{m} (\lfloor \sqrt[3]{m} \rfloor - \lfloor \sqrt[3]{k} \rfloor)$ to our original sum. As

$$\sum_{k=0}^{m} \lfloor \sqrt[3]{m} \rfloor = \lfloor \sqrt[3]{m} \rfloor \sum_{k=0}^{m} 1 = \lfloor \sqrt[3]{m} \rfloor (m+1),$$

we can finally conclude

$$\sum_{k=0}^{m} \lfloor \sqrt[3]{k} \rfloor = \sum_{k=0}^{m} \lfloor \sqrt[3]{m} \rfloor - \sum_{k=0}^{m} f(k) = \lfloor \sqrt[3]{m} \rfloor (m+1) - \frac{\lfloor \sqrt[3]{m} \rfloor^2 (\lfloor \sqrt[3]{m} \rfloor + 1)^2}{4}.$$

**Prob 2.** (a) Find a recurrence relation for the balance $B(k)$ owed at the end of $k$ months on a loan at a rate $r$ if a payment $P$ is made on the loan each month.

**Solution:** We need to apply interest to our previous balance and subtract our fixed payment. This gives

$$B(k) = B(k-1)\Big(1 + \frac{r}{12}\Big) - P. \tag{2}$$

Note that the interest is computed using the monthly rate, i.e., 1/12 of the annual interest rate.

(b) Determine what the monthly payment $P$ should be so that the loan is paid off after $T$ months.

**Solution:** Iterate the recurrence (2) $k-1$ times, i.e., keep replacing each balance $B(k-j)$ by the previous balance $B(k-j-1)$ using the recurrence (2) for $j = 1, \ldots, k-1$. This produces

$$B(k) = B(0)\Big(1 + \frac{r}{12}\Big)^k - P - P\Big(1 + \frac{r}{12}\Big) - P\Big(1 + \frac{r}{12}\Big)^2 - \cdots - P\Big(1 + \frac{r}{12}\Big)^{k-1}.$$

The subtracted part is the sum of a geometric progression with ratio $1 + r/12$ and initial term $P$, i.e.,

$$P\frac{(1+\frac{r}{12})^k - 1}{(1 + \frac{r}{12} - 1)} = \frac{12P}{r}\big((1 + \frac{r}{12}\big)^k - 1\big), \quad \text{so} \qquad B(k) = (B(0) - \frac{12P}{r})\Big(1 + \frac{r}{12}\Big)^k + \frac{12P}{r}.$$

To pay the loan off after $T$ months, we must have $B(T) = 0$, i.e.,

$$P = \frac{rB(0)}{12} \cdot \frac{\Big(1 + \frac{r}{12}\Big)^T}{\Big(1 + \frac{r}{12}\Big)^T - 1}.$$

(c) Suppose you take out a fixed-rate mortgage for $\$1M$ at the current (historically low) rate 3% and want to pay it off in 20 years. What monthly payment should you make?

**Solution:** Plug in $r = .03$, $T = 20 \cdot 12 = 240$, and $B(0) = 1000000$ to get

$$P = 2500 \cdot \frac{1.0025^{240}}{1.0025^{240} - 1} \approx 5545.97$$

So the fixed payment should be about $\$5,546$ per month.

(d) Now suppose the same mortgage of $\$1M$ but you have qualified only for the rate 5% and the maximum monthly payment you can afford is \$5K. How many years will it take you to pay off that mortgage?

**Solution:** Now we must have

$$\Big(\frac{12P}{r} - B(0)\Big)\Big(1 + \frac{r}{12}\Big)^T = \frac{12P}{r}, \qquad \text{hence} \qquad \Big(1 + \frac{r}{12}\Big)^T = \frac{12P}{12P - rB(0)},$$

which yields

$$T = \frac{\ln(12P) - \ln(12P - rB(0))}{\ln\Big(1 + \frac{r}{12}\Big)}.$$

Plugging in our new data $P = 5000$, $r = 0.05$, $B(0) = 1000000$, we get

$$T = \frac{\ln 6}{\ln 1.00416667} \approx 430.918$$

This is time in months, and conversion into years gives approximately 35.9 years.

**Prob 3.** Write down the full addition and multiplication tables for $\mathbb{Z}_9$ (where addition means $+_9$ and multiplication means $\cdot_9$).

**Solution:**

| $+_9$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 8 | 8 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

| $\cdot_9$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 2 | 0 | 2 | 4 | 6 | 8 | 1 | 3 | 5 | 7 |
| 3 | 0 | 3 | 6 | 0 | 3 | 6 | 0 | 3 | 6 |
| 4 | 0 | 4 | 8 | 3 | 7 | 2 | 6 | 8 | 5 |
| 5 | 0 | 5 | 1 | 6 | 2 | 7 | 3 | 8 | 4 |
| 6 | 0 | 6 | 3 | 0 | 6 | 3 | 0 | 6 | 3 |
| 7 | 0 | 7 | 5 | 3 | 8 | 8 | 6 | 4 | 2 |
| 8 | 0 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

**Prob 4.** (a) Prove that, if $p$ is a prime, then all positive integers less than $p$ except for 1 and $p-1$ can be split into $(p-3)/2$ pairs such that each pair consists of integers that are inverses of each other modulo $p$.

**Proof.** For $p = 2$, the proof of this fact is vacuous.

Suppose $p > 2$. Then $p$ is necessarily odd. If $a$ is relatively prime to $p$, the congruence $ax \equiv 1 \pmod{p}$ has a unique solution $x \in \{1, \ldots, p-1\}$. Each number in the set $S = \{2, 3, \ldots, p-2\}$ is relatively prime to $p$, hence has a unique inverse mod $p$; that inverse lies in the same set $S$ because the numbers 1 and $p-1$ are their own multiplicative inverses.

Moreover, there are no elements of $S$ that are multiplicative inverses of themselves, since the congruence $k^2 \equiv 1 \pmod{p}$ implies $p|(k^2-1)$, i.e., $p|(k-1)(k+1)$. Since $p$ is prime, this implies that $p|(k-1)$ or $p|(k+1)$, so $k \equiv \pm 1 \pmod{p}$, and the latter condition is not met by any element of $S$.

Thus the set $S$ splits into $(p-3)/2$ pairs that are inverses of each other.

(b) Conclude from part (a) that $(p-1)! \equiv -1 \pmod{p}$ whenever $p$ is prime.

**Proof.** From (a), we see that the product of all numbers in the set $S$ is congruent to 1 mod $p$ because it can be rewritten as a product of $(p-3)/2$ pairs that are inverses of each other mod $p$. Now,

$$(p-1)! = 1\Big(\prod_{j \in S} j\Big)(p-1) \equiv 1(-1) \equiv -1 \pmod{p}.$$

(c) What can we conclude if $n$ is a positive integer such that $(n-1)! \not\equiv -1 \pmod{n}$?

If $(n-1)! \not\equiv -1 \pmod{n}$, this shows $n$ is composite: if $n$ were prime, that congruence would hold by (b).

**Prob 5.** Prove or disprove that there are infinitely many primes of the form $6k+5$, $k \in \mathbb{Z}_+$.

**Proof.** Suppose there are only finitely many primes of the form $6k+5$. List all them as $p_1$, $p_2$, …, $p_n$ for some $n \in \mathbb{N}$. Consider the number $N = 6p_1 \cdots p_n - 1$. This is a number of the form $6k+5$ as well, since $N = 6(p_1 \cdots p_n - 1) + 5$. None of the primes $p_1$, …, $p_n$ divides $N$ since $N \equiv -1 \pmod{p_j}$ for all $j = 1, \ldots, n$. $N$ is either prime or composite.

If $N$ is prime, then $N$ is not on the original list $(p_j)_{j=1}^n$ since none of the $p_j$s even divides $N$.

If $N$ is composite, consider its prime divisors. $N$ is not divisible by 2 or 3 since $N \equiv -1 \pmod 6$. A prime cannot be of the form $6k$, $6k+2$, $6k+3$ or $6k+4$ for $k \in \mathbb{N}$ since these expressions can all be explicitly divided by 2 or by 3 and are greater than those two numbers.

Hence all prime divisors of $N$ are either $-1$ or 1 mod 6. If they were all equal to 1 mod 6, then $N$ itself would also be equal to 1 mod 6, but $N \equiv -1 \pmod 6$. Hence at least one of the prime divisors of $N$ is equal to $-1 \equiv 5 \pmod 6$. We already established that no prime divisor of $N$ is on the original list $(p_j)_{j=1}^n$. Hence we have found a new prime of the form $6k+5$.

Thus, we have established that there are infinitely many primes of the form $6k+5$.