Number Theory Homework

Question 1:

Prove by mathematical induction that

$$1 + 2 + \ldots\ldots\ldots\ldots\ldots + m = \frac{m(m+1)}{2}$$

Solution:

Step 1: Technique of Induction

Mathematical induction proves by checking if a proposition hold's for m=1, and m= k+1 whenever it holds for m=k, then the proposition holds for all positive integers m= 1,2, 3,........

Step 2: Substitute m=1 in the equation:

$$1 = \frac{1(1+1)}{2} = 1$$

Step 3: Assume that the formula holds for m= k

$$1 + 2 + \ldots\ldots\ldots\ldots\ldots + k = \frac{k(k+1)}{2}$$

Step 4: Proof that the formula holds for $m = k+1$.

$$1 + 2 + \ldots\ldots\ldots\ldots\ldots + k + (k+1) = \frac{(k+1)\{(k+1)+1\}}{2}$$

$$1 + 2 + \ldots\ldots\ldots\ldots\ldots + k = \frac{k(k+1)}{2}$$

$$\Rightarrow \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)\{(k+1)+1\}}{2} \Rightarrow \frac{k(k+1)+2k+2}{2} = \frac{(k+1)\{(k+2)}{2}$$

$$\Rightarrow \frac{(k+1)\{(k+2)}{2} = \frac{(k+1)\{(k+2)}{2}$$ {by factorization}

Proved

Question 2:

Prove by induction that for every positive integer n, then:

$1^2 + 2^2 + 3^2 + 4^2 + \ldots\ldots\ldots\ldots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$

Solution:

Step 1: Technique of Induction

Mathematical induction proves by checking if a proposition hold's for $n = 1$, and $n = k + 1$ whenever it holds for $n = k$, then the proposition holds for all positive integers n= 1,2, 3,........

Step 2: Substitute $n = 1$ in the equation:

$1 = \dfrac{1\{1+1\}\{(2\times1)+1\}}{6} = 1$

Step 3: Assume that the formula holds for k

$1^2 + 2^2 + 3^2 + 4^2 + \ldots\ldots\ldots\ldots + k^2 = \dfrac{k(k+1)(2k+1)}{6}$

Step 4: Proof that the formula holds for n= k+1.

$1^2 + 2^2 + 3^2 + 4^2 + \ldots\ldots\ldots\ldots + (k+1)^2 = \dfrac{(k+1)(k+1+1)\{2(k+1)+1\}}{6}$

$1^2 + 2^2 + 3^2 + 4^2 + \ldots\ldots\ldots\ldots + (k+1)^2 = (1^2 + 2^2 + 3^2 + 4^2 + \ldots\ldots\ldots\ldots + k^2) + (k+1)^2$

$\Rightarrow \dfrac{k(k+1)(2k+1)}{6} + (k+1)^2$

$\Rightarrow \dfrac{(k+1)(2k^2+k+6k+6)}{6} \Rightarrow \dfrac{(k+1)(k+2)(2k+3)}{6}$ {by factorization}

Proved

Question 3:

Find the LCM of 16, 24 and 840.

Solution:

STEP 1*:* Express each of the numbers as prime factors

$16 = 2^4$

$24 = 2^3 \times 3$

$840 = 2^3 \times 3 \times 5 \times 7$

STEP 2: Pick out the highest power of each of the prime factors that appears. The factors need not be common. For example, the highest powers of 2,3 ,5 and 7 are 4,1, 1, and the LCD becomes $2^4\times3\times5\times7=1680$.

Question 4:

Solve the Diophantine equation

$2772x + 390y = (2772,390)$

Solution:

STEP 1: Applying the Euclidean algorithm to find gcd of 2772 and 390

$\Rightarrow$ 2772 = 7 × 390 + 42……………………………………(i)

$\Rightarrow$ 390 = 9 × 42 + 12………………………………………(ii)

$\Rightarrow$ 42 = 3 × 12 + 6…………………………………………(iii)

The gcd = 6

STEP 2: Substitute the gcd in the equation ie 2772x + 390y = 6

Substitute backwards in (iii), then (ii) and finally in (i) to obtain solutions for the Diophantine

$\Rightarrow$ 6 = 42 – 3 × 12

$\Rightarrow$ = 42 – 3 × (390 – 9 × 42) = 42 – 3(390)

$\Rightarrow$ = 42 + 27(42) – 3(390)

$\Rightarrow$ = 28(42) – 3(390)

$\Rightarrow$ = 28(2772 – 7 × 390) – 3(390)

$\Rightarrow$ = 28 (2772) – 196(390) – 3(390)

$\Rightarrow$ = 28(2772) – 199(390)

i.e. ($mx + ny$)

Hence, $x = 28$, $y = {}^{-}199$

Question 5:

List down Pythagoras Triplets

Solution:

(a, b, c)	(a, b, c)	(a, b, c)	(a, b, c)
3,4,5	64,1023,1025	84,13,85	96,2303,2305
5,12,13,	68,285,293	84,187,205	100,621,629
7,24,25	63,1155,1157	84,437,445	100,2499,2501
9,40,41	72,65,97	84,1763,1765	
15,8,17	72,1295,1297	88,105,137	

21,20,29	76,357,365	88,1935,1937	
35,12,37	76,1443,1445	92,525,533	
45,28,53	80,39,89	92,2115,2117	
63,16,65	80,1599,1601	96,247,265	

Question 6:

Solve 105x + 28y = 14. We know that hcf(105, 28) = 7 and also that 7|14 and so a solution exists. Recall that 105·(−1)+28·4 = 7 and so 105·(−2)+28·8 = 14. So (x0, y0) = (−2, 8) is a solution.

Solution:

Let (x_0, y_0) be a solution. Then (x, y) solves $(\star)$ iff $a(x-x_0)+b(y-y_0)=0$ that is iff $u=x-x_0$, $v=y-y_0$ solve $au+bv=0$ $(\star\star)$. Write $d=\text{hcf}(a,b)$ and $a=da'$, $b=db'$. Then $(\star\star)$ is equivalent to $a'u+b'v=0$ where $\text{hcf}(a',b')=1$. Note that now $a'|v$, i.e. $v=ka'$ and so $u=-kb'$. That is, u, v solves $(\star\star)$ iff $u=-kb'$ and $v=ka'$ for some $k\in\mathbb{Z}$. Therefore the solutions to $(\star)$ are

$$\{x=x_0-kb',\ y=y_0+ka' \mid k\in\mathbb{Z}\}.$$

Question 7:

Proof of the finiteness of certain complete systems of functions

Solution:

In the theory of algebraic invariants, questions as to the finiteness of complete systems of forms deserve, as it seems to me, particular interest. L. Maurer has lately succeeded in extending the theorems on finiteness in invariant theory proved by P. Gordan and myself, to the case where, instead of the general projective group, any subgroup is chosen as the basis for the definition of invariants.

An important step in this direction had been taken al ready by A. Hurwitz, who, by an ingenious process, succeeded in effecting the proof, in its entire generality, of the finiteness of the system of orthogonal invariants of an arbitrary ground form.

The study of the question as to the finiteness of invariants has led me to a simple problem which includes that question as a particular case and whose solution probably requires a decidedly more minutely detailed study of the theory of elimination and of Kronecker's algebraic modular systems than has yet been made.

Let a number *m* of integral rational functions $X_1, X_2, \dots, X_m$ of the *n* variables $x_1, x_2, \dots, x_n$ be given,

$$(S)\qquad \begin{aligned} X_1 &= f_1(x_1, \dots, x_n) \\ X_2 &= f_2(x_1, \dots, x_n) \\ &\dots\dots \\ X_m &= f_m(x_1, \dots, x_n) \end{aligned}$$

Every rational integral combination of $X_1, \dots, X_m$ must evidently always become, after substitution of the above expressions, a rational integral function of $x_1, \dots, x_n$. Nevertheless, there may well be rational fractional functions of $X_1, \ldots, X_m$ which, by the operation of the substitution *S,* become integral functions in $x_1, \ldots, x_n$.

Every such rational function of $X_1, \ldots, X_m$, which becomes integral in $x_1, \ldots, x_n$ after the application of the substitution *S,* I propose to call a *relatively integral* function of $X_1, \ldots, X_m$. Every integral function of $X_1, \ldots, X_m$ is evidently also relatively integral; further the sum, difference and product of relative integral functions are themselves relatively integral.

The resulting problem is now to decide whether it is always possible *to find a finite system of relatively integral function* $X_1, \ldots, X_m$ *by which every other relatively integral function of* $X_1, \ldots, X_m$ *may be expressed rationally and integrally.*

We can formulate the problem still more simply if we introduce the idea of a finite field of integrality. By a finite field of integrality I mean a system of functions from which a finite number of functions can be chosen, in terms of which all other functions of the system are rationally and integrally expressible. Our problem amounts, then, to this: to show that all relatively integral functions of any given domain of rationality always constitute a finite field of integrality.

It naturally occurs to us also to refine the problem by restrictions drawn from number theory, by assuming the coefficients of the given functions $f_1, \ldots, f_m$ to be integers and including among the relatively integral functions of $X_1, \ldots, X_m$ only such rational functions of these arguments as become, by the application of the substitutions *S,* rational integral functions of $x_1, \ldots, x_n$ with rational integral coefficients.

The following is a simple particular case of this refined problem: Let *m* integral rational functions $X_1, \ldots, X_m$ of one variable *x* with integral rational coefficients, and a prime number *p* be given. Consider the system of those integral rational functions of *x* which can be expressed in the form

$$\frac{G(X_1, \ldots, X_m)}{p^h},$$

where *G* is a rational integral function of the arguments $X_1, \ldots, X_m$ and p^h is any power of the prime number *p.* Earlier investigations of mine show immediately that all such expressions for a fixed exponent *h* form a finite domain of integrality. But the question here is whether the same is true for all exponents *h, i. e.,* whether a finite number of such expressions can be chosen by means of which for every exponent *h* every other expression of that form is integrally and rationally expressible.

From the boundary region between algebra and geometry, I will mention two problems. The one concerns enumerative geometry and the other the topology of algebraic curves and surfaces.