4^{th} International Tournament of Young Mathematicians

Belarus

Problem 2. Number of Residues

Abstract

This problem is about calculating the cardinal of the value set over modulo (V_f^n) of integer-valued polynomials and in particular the value set of triangular numbers. At the beginning of the paper we studied some properties of integer-valued polynomials. Next we provided the exact formula to calculate the value set of arbitrary integer-valued polynomial (question 4), and proved that $\#V_f^n$ is a multiplicative with respect to modulo function.

Thus we have the formula to compute the value set, in practice it's very complex and need too much calculations, and using formula we can't find the value set itself, so we also investigated more efficient algorithms to find and hence compute the value set. Also we studied bounds for the value set.

In some particular cases of polynomials we can find explicit formulas for $\#V_f^n$. We provided such formulas for monomials, arbitrary linear and quadratic polynomials over arbitrary modulo (which in particular solved questions 1 - 3).

In the last part we considered generalizations of the problem, we investigated rational functions taking integer values in integer points and linear functions of several variables.

Contents

Definitions and initial statement

The initial statement of the problem was the following:

- Questions 1-3. Calculate the value set of triangular numbers $f(x) = \frac{x(x+1)}{2}$ over modulo.
- Question 4. Calculate the value set of arbitrary integer-valued polynomial over modulo.
- Question 5. Suggest and investigate related problems.

For comfort we'll have some definitions:

Definition 1. Denote by V_f^n the set of values that function f may take over modulo n and $\#V_f^n$ is the cardinality of V_f^n.

Definition 2. Denote by S_f^n number of solutions to the congruence $f(x) \equiv 0 \pmod{n}$.

Definition 3. Let $\mathrm{Int}(\mathbb{Z})$ be the set of all polynomials with real coefficients taking integer values in any integer point.

1 Introduction

In this section we study properties of integer-valued polynomials and properties of value set cardinality needed for further research.

1.1 Classification of integer-valued polynomials

Theorem 1. *Every polynomial $f \in Int(\mathbb{Z})$ can be represented in the form*

$$f(x) = \sum_{k=0}^{m} t_k \binom{x}{k}$$

where $m = \deg f$ and $t_k \in \mathbb{Z}$. □

It's easy to see that polynomials $\binom{x}{k}$ are integer-valued. Since there exists exactly one polynomial $\binom{x}{k}$ of each degree, then any polynomial from $\mathbb{R}[x]$ and the more from $\mathrm{Int}(\mathbb{Z})$ can be represented in form:

$$f(x) = \sum_{i=0}^{m} t_i \binom{x}{i} = t_m \binom{x}{m} + \cdots + t_1 \binom{x}{1} + t_0, \tag{1}$$

where $t_i \in \mathbb{R}$ and $m = \deg f$.

Show by induction on k that if $f \in \mathrm{Int}(\mathbb{Z})$ then $t_k \in \mathbb{Z}$. We have $f(0) = t_0 \in \mathbb{Z}$. Suppose $t_i \in \mathbb{Z}$ holds for all $i \leq k$. Then $f(k+1) = \sum_{i=0}^{m} t_i \binom{k+1}{i}$. For $i > k+1$ there holds $\binom{k+1}{i} = 0$, hence $f(k+1) = \sum_{i=0}^{k+1} t_i \binom{k+1}{i} = t_{k+1} + \sum_{i=0}^{k} t_i \binom{k+1}{i} \in \mathbb{Z}$. As $f(k+1) \in \mathbb{Z}$ and $\sum_{i=0}^{k} t_i \binom{k+1}{i} \in \mathbb{Z}$ we have $t_{k+1} \in \mathbb{Z}$. ■

1.2 Properties of integer-valued polynomials

Proposition 1.1. *Integer-valued polynomial $f \in Int(\mathbb{Z})$ of degree $d = \deg f$ takes all possible values modulo n on numbers $0, 1, \ldots, nd! - 1$.*

□ To prove it show that $f(x) \equiv f(x + nd!) \pmod{n}$. From theorem 1 there holds $f = t_d\binom{x}{d} + \cdots + t_1\binom{x}{1} + t_0$ for some integer t_i. Consider the difference

$$f(x + nd!) - f(x) =$$

$$= t_d\binom{x + nd!}{d} - t_d\binom{x}{d} + \cdots + t_1\binom{x + nd!}{1} - t_1\binom{x}{1} + t_0(1 - 1) = \tag{2}$$

$$= \frac{t_d}{d!}\Big((x + nd!)...(x + nd! - d + 1) - x(x - 1)...(x - d + 1)\Big) + \cdots + t1(x + nd! - x).$$

Each summand is of the form $\frac{t_i}{i!}\big(A - B\big)$, where $A = (x + nd!)...(x + nd! - i + 1)$ and $B = x(x - 1)...(x - i + 1)$. Note that after removing the brackets each element from B will also be in A multiplied by -1, and each element from A that is not in B will be multiplied by $nd!$. Thus $\frac{t_i}{i!}\big(A - B\big)$ can be written in the form $\frac{t_i}{i!}\big(Cnd!\big) = t_iCnd(d - 1)...(d - i + 1) \equiv 0 \pmod{n}$. So $f(x + nd!) - f(x) \equiv 0 \pmod{n}$. ■

Proposition 1.2. To calculate the cardinal of the value set of $f(x) \in \mathrm{Int}(\mathbb{Z})$ over modulo n, it's the same that to calculate the cardinal of the value set of $df(x)$ with $d \in \mathbb{Z}$ over modulo dn, where d is the smallest positive integer such that all coefficients of f are integers (and from theorem 1 follows $d \mid (\deg f)!$).

2 Exact value for $\#V_f^n$

In this section we provide explicit formula to calculate the value set and prove that $\#V_f^n$ is multiplicative with respect to modulo function.

2.1 Exact formula

From proposition 1.2 for every integer-valued polynomial there exists a polynomial with integer coefficients with the same cardinal of the value set. So we consider polynomials with integer coefficients.

Theorem 2. *Let $f \in \mathbb{Z}[x]$ and $n \in \mathbb{N}$, then the following holds:*

$$\#V_f^n = n\sum_{u=0}^{n-1}\left(\sum_{v=0}^{n-1}\sum_{t=0}^{n-1}\exp\left[2\pi i\frac{t}{n}\big(f(u) - f(v)\big)\right]\right)^{-1} * \tag{3}$$

*brackets [...] just for clarity

□ To prove the formula we'll use basic knowledge of graph theory. It's clear that the polynomial takes all it values in points $0, \dots, n-1$. Consider an undirected graph with vertices as residues modulo n and edge between u and v means $f(u) = f(v)$. Note that it consists of several connected components and each of them is complete. The number of components is the cardinality of the value set of f. To calculate the number of components (i.e. $\#V_f^n$) we can set in each vertex u the value which equal to the cardinal of component containing u powered -1, thus sum of values will be equal to $\#V_f^n$. Or it can be written as:

$$\#V_f^n = \sum_{u=0}^{n-1} \left(\sum_{v: f(u)-f(v)=0} 1 \right)^{-1} = n \sum_{u=0}^{n-1} \left(\sum_{v: f(u)-f(v)=0} n \right)^{-1} \tag{4}$$

Show that sum $\sum_{v:f(u)-f(v)=0} n$ can be rewritten in the form $\sum_{v=0}^{n-1} \sum_{t=0}^{n-1} \exp\left[2\pi i \frac{t}{n}\big(f(u)-f(v)\big)\right]$. If $f(u)-f(v) \neq 0$, then $\exp\left[2\pi i \frac{1}{n}\big(f(u)-f(v)\big)\right] \neq 1$, thus this sum is sum of first n members of geometric progression with ratio $r = \exp\left[2\pi i \frac{1}{n}\big(f(u)-f(v)\big)\right]$ and first member $a = \exp\left[2\pi i \frac{0}{n}\big(f(u)-f(v)\big)\right] = e^0 = 1$. Hence this sum equals

$$a\frac{r^n - 1}{r-1} = \frac{e^{2\pi i \left(f(u)-f(v)\right)} - 1}{e^{2\pi i \frac{1}{n}\left(f(u)-f(v)\right)} - 1} = \Big[\text{as } \big(f(u)-f(v)\big) \text{ is integer}\Big] = 0 \tag{5}$$

In case when $f(u) - f(v) = 0$, $\exp\left[2\pi i \frac{t}{n}\big(f(u)-f(v)\big)\right] = 1$ and then $\sum_{t=0}^{n-1} \exp\left[2\pi i \frac{t}{n}\big(f(u)-f(v)\big)\right] = n$. Thus we have:

$$\#V_f^n = n \sum_{u=0}^{n-1} \left(\sum_{v=0}^{n-1} \sum_{t=0}^{n-1} \exp\left[2\pi i \frac{t}{n}\big(f(u)-f(v)\big)\right] \right)^{-1} . \blacksquare$$

2.2 Multiplicativity

Theorem 3. *Let $f(x) \in \mathbb{Z}[x]$ and $n \in \mathbb{N}$, then $\#V_f^n$ is multiplicative with respect to n function.*

□ By definition $\#V_f^n$ is defined for every natural n and $\#V_f^1 = 1$. Let $n = p * q$ with $(p, q) = 1$, show that $\#V_f^n = \#V_f^p * \#V_f^q$. Consider mapping ϕ: $V_f^p \times V_f^q \to \mathbb{Z}_{pq}$ as the following $\phi(a, b) = c$ where c is the solution to the system

$$\begin{cases} a \equiv c \pmod{p} \\ b \equiv c \pmod{q} \end{cases}$$

by Chinese remainder theorem there exists exactly one such c. For each pair $(a, b), a \in V_f^p, b \in V_f^q$ there exist $x \in \mathbb{Z}_p, y \in \mathbb{Z}_q$ such that $\big(a, b\big) = \big(f(x), f(y)\big)$. So by Chinese remainder theorem there exists $z \in \mathbb{Z}_{pq}$ which is solution to

$$\begin{cases} x \equiv z \pmod{p} \\ y \equiv z \pmod{q} \end{cases}$$

As f is a polynomial with integer coefficients and $f(t) \equiv f(t+m) \pmod{m}$ then $f(z) \equiv f(x) \equiv a \pmod{p}$ and $f(z) \equiv f(y) \equiv b \pmod{q}$. Therefore $f(z) \equiv c \pmod{pq}$. So $c \in V_f^{pq} = V_f^n$ and ϕ is a mapping to V_f^n.

By Chinese remainder theorem for each c there exists a preimage $\phi^{-1}(c)$, so ϕ is a surjection and $\phi((u_1, v_1)) = \phi((u_2, v_2))$ implies $(u_1, v_1) = (u_2, v_2)$, so ϕ is an injection. Therefore ϕ is a bijection. Hence $\#V_f^{pq} = \#V_f^p * \#V_f^q$, thus $\#V_f^n$ is a multiplicative function. ■

Corollary 3.1. If $n = p_1^{\alpha_1} * \cdots * p_k^{\alpha_k}$, then to calculate $\#V_f^n$ it's enough to calculate $\#V_f^{p_i^{\alpha_i}}$ for all i and multiply the values.

3 Algorithms to find the value set

Despite the fact that theorem 3 provides explicit formula to calculate the value set, in practice this formula is very complex and for $d = \deg f$ and modulo q needs $O(d*q^3)$ simple operations to be computed. In this section we suggest more efficient ways to find (and hence calculate) the value set over modulo. From corollary 3.1 we assume that the value set is calculated over prime power $q = p^m$, which in practice significantly accelerates algorithms.

3.1 Naive algorithm

Proposition 4. *The value set of a polynomial of degree d over modulo $q = p^m$ can be found in $O(d * p^m)$.*

□ This can be done using very simple algorithm. For every $x \in \mathbb{Z}_q$ we calculate the value of $f(x)$ over modulo q and memorize it. Then for every $y \in \mathbb{Z}_q$ we check whether y was memorized. Obviously this algorithm will find the value set. There are $O(p^m)$ in $\mathbb{Z}_{p^m}$ and each value is calculated in $O(d)$ and memorized and checked in $O(1)$. So total runtime is $O(p^m) * O(d) + O(p^m) * O(1) = O(p^m * d) + O(p^m) = O(d * p^m)$. ■

3.2 Lifting algorithm

To provide more efficient algorithm we'll use a result known as Hensel's lemma [4]:

Hensel's lemma. *If $a \in \mathbb{Z}_{p^e}$ is a solution to $f(x) \equiv 0 \pmod{p^e}$, then, where $f'(x)$ is the derivative of f, this solution lifts to a solution to $f(x) \equiv 0 \pmod{p^{e+1}}$, depending on whether $p \mid f'(a)$ and $p^{e+1} \mid f(a)$:*

- *if $p \nmid f'(a)$, then $f(x) \equiv 0 \pmod{p^{e+1}}$ has the unique solution $x \equiv a + tp^e \pmod{p^{e+1}}$ where t is unique solution to the linear congruence*

$$tf'(a) \equiv -\frac{f(a)}{p^e} \pmod{p};$$

- *if $p \mid f'(a)$ and $p^{e+1} \mid f(a)$ then $f(x) \equiv 0 \pmod{p^{e+1}}$ has p distinct solutions of the form $x \equiv a + tp^e \pmod{p^{e+1}}$ with $t = 0, \ldots, p-1$;*
- *if $p \mid f'(a)$ and $p^{e+1} \nmid f(a)$ then $f(x) \equiv 0 \pmod{p^{e+1}}$ has no solutions which reduce to $a \pmod{p^e}$;*

Lemma 5. *A polynomial congruence $f(x) = a_d x^d + \cdots + a_1 x + a_0 \equiv 0 \pmod{p^m}$ can be solved in $O\big(p + S_f^{p^m} + d\sum_{i=1}^{m-1} S_f^{p^i}\big)$.*

□ The algorithm to solve the congruence have m steps. On step i (counting from 0) we have the set of solutions to $f(x) \equiv 0 \pmod{p^i}$.

Initially we have one solution $x \equiv 0 \pmod 1$. On first step we try all the numbers $0, \ldots, p-1$ to be the solution of $f(x) \equiv 0 \pmod p$. On each other step we use Hensel's Lifting lemma, and from each solution modulo p^i we lift solutions to $\pmod{p^{i+1}}$. Finally we'll have solutions modulo p^m.

On each step despite the first for each solution we find solutions by the higher power of p in $O(d)$ operations, by calculating the values of f and f'. On first step we have $O(p)$ operations.

Thus totally there are $O\big(p + S_f^{p^m} + d\sum_{i=1}^{m-1} S_f^{p^i}\big)$ operations. ■

The algorithm, we provide is more effective than the trivial one for polynomials with $V_f^n < \min(p, d)$.

Theorem 6. *The value set of a polynomial f of degree d over modulo p^m can be found in $O\big(p * \#V_f^{p^m} + \#V_f^{p^m} * p^m + d * p^{m-1} * \#V_f^{p^m}\big)$.*

□ The idea is not to consider residues, which values are already in the value set. We'll have two types of marks for residues of $\mathbb{Z}_{p^m}$, mark of first type to show that a is in the value set, and mark of second type to show that we have no need to consider a.

Let step over all elements of $\mathbb{Z}_{p^m}$ from 0 to $p^m - 1$. Suppose a is considered. If a is marked with second type mark, we skip a and go to the next step.

If a is not marked, we make a mark of first type on $f(a)$, to memorize that $f(a)$ is in the value set. Then we solve polynomial congruence $f(x) - f(a) \equiv 0 \pmod{p^m}$. Roots of the congruence if the elements of $\mathbb{Z}_{p^m}$ which have the same value as $f(a)$ (including a itself). So we mark all the roots with the second mark and go to the next step.

In the end of the algorithm the value set if numbers marked with first-type mark.

Totally the algorithm have p^m steps. And there are $\#V_f^{p^m}$ steps which is not skipped (i.e. not in $O(1)$). On each such step we calculate the value of f which is $O(d)$ and we solve the congruence, which is $O\big(p + S_g^{p^m} + d\sum_{i=1}^{m-1} S_f^{p^i}\big)$. As we consider every value from the value set only one time, sum of all considered roots of congruences $S_g^{p^m}$ is $O(p^m)$. In the sum $\sum_{i=1}^{m-1} S_f^{p^i}$ there holds $S_f^{p^i} \le p^i$, hence sum of all such sums is $O(\#V_f^{p^m} \sum_{i=1}^{m-1} p^i) = \#V_f^{p^m} * p^{m-1})$. Thus total asymptotic is

$$O\big(\#V_f^{p^m} * p + \sum_{t \in V_f^{p^m}} S_{f(x)-f(t)}^{p^m} + d * \#V_f^{p^m} * p^{m-1}\big) =$$

$$O\big(p * \#V_f^{p^m} + \#V_f^{p^m} * p^m + d * p^{m-1} * \#V_f^{p^m}\big). ■$$

4 Bounds for $\#V_f^n$

4.1 Bounds for product of primes

Proposition 7. *For $f(x) \in \mathbb{F}_p[x]$, $d = \deg f$ there holds $\frac{p}{d} \leq \#V_f^p \leq p$.*

□ It's clear that $\#V_f^p \leq p$ since there p elements in the field.

As $\mathbb{F}_p$ is a field a polynomial in $\mathbb{F}_p[x]$ of degree $\deg f = d$ can have at most d roots. So for every $\alpha \in V_f^p$ there exist at most d such β that $f(\beta) = \alpha$. And as all such roots β to $f(\beta) = \alpha$ for all $\alpha \in V_f^p$ form the field, we have:

$$p \leq \#V_f^p * d \iff \#V_f^p \geq \frac{p}{d}.\blacksquare \tag{6}$$

Corollary 7.1. Since $\#V_f^n$ is multiplicative function then for modulo equal product of primes $n = p_1 * p_2 * \cdots * p_k$ there holds:

$$\frac{p_1 * p_2 * \cdots * p_k}{d^k} \leq \#V_f^n \leq n.$$

5 Particular cases

In this part we obtain better or more explicit results for $\#V_f^q$ in some particular cases of polynomials. Using proposition 1.2 we suppose that polynomial f have integer coefficients, and using corollary 3.1 we suppose that modulo is power of prime $q = p^m$.

Lemma 8. *Linear transformation $g(x) = ax + b$ maps set of residues $T \subset \mathbb{Z}_m$ into the set with the same cardinal, if $(a, m) = 1$.*

■ It's enough to show that $g(x)$ are different for all $x \in T$. Assume a contrary, let there exist u and v, such that $u \not\equiv v \pmod{m}$ and $g(u) \equiv g(v) \pmod{m}$. Then we have: $au + b \equiv av + b \pmod{m} \iff au \equiv av \pmod{m}$. As $(a, m) = 1$ by Euler's theorem there exists element a^{-1}. Hence $a^{-1}au \equiv a^{-1}av \pmod{m} \iff u \equiv v \pmod{m}$ which is false by assumption, therefore assumption is wrong. □

Corollary 8.1. For linear transformation $g(x) = ax + b$ with $(a, m) = 1$ there holds $V_{f \circ g}^m = V_f^m$, since the set of residues is mapped into itself.

5.1 Monomials

Theorem 9. *Let $f(x) = x^d$, and $p \geq 3$ be a prime, $m \in \mathbb{N}$ and $1 \leq k \leq d$ and $k \equiv m \pmod{d}$, then*

$$\#V_f^{p^m} = \frac{(p-1)}{(d, (p-1)p^{k+d-1})} \left(p^{k+d-1} \left(\frac{p^{d\left\lfloor \frac{m-1}{d} \right\rfloor} - 1}{p^d - 1} \right) \right) + \frac{(p-1)p^{k-1}}{(d, (p-1)p^{k-1})} + 1 \tag{7}$$

□ Consider congruence $x^d \equiv a \pmod{p^m}$. Let g be some primitive root over modulo p^m, since p is a prime ≥ 3 such primitive root exists [1]. If $(a, p^m) = 1$ then there exists a number $\mathrm{ind}_g a$, such that $g^{\mathrm{ind}_g a} = a$. Hence

$$\mathrm{ind}_g x^d \equiv \mathrm{ind}_g a \pmod{\varphi(p^m)} \iff d\ \mathrm{ind}_g x \equiv \mathrm{ind}_g a \pmod{\varphi(p^m)} \tag{8}$$

Solution to this congruence exists if and only if $\big(d, \varphi(p^m)\big) \mid \mathrm{ind}_g a$. Clearly there exist exactly

$$\frac{\varphi(p^m)}{\big(d, \varphi(p^m)\big)}$$

such numbers. So $f(x) = x^d$ takes exactly $\frac{\varphi(p^m)}{\big(d,\varphi(p^m)\big)}$ values which are coprime to p^m.

Consider values which are not coprime to p^m. Let $m > d$ and $x^d \equiv t \pmod{p^m}$, with $t \,\vdots\, p$. Then $x \,\vdots\, p \iff x^d \,\vdots\, p^d \iff t \,\vdots\, p^d$. Hence the congruence $x^d \equiv t \pmod{p^m}$ has the same number of solutions that the congruence $(x')^d \equiv t' \pmod{p^{m-d}}$.

Let $m \leq d$ and $x^d \equiv t \pmod{p^m}$, with $t \,\vdots\, p$. Then $x \,\vdots\, p \iff x^d \,\vdots\, p^d \iff t \,\vdots\, p^d \iff t \equiv 0 \pmod{p^m}$. So in these case there exists exactly one number from value set which is divided by p. Therefore we can calculate $\#V_f^{p^m}$ recursively

$$\#V_f^{p^m} = \frac{\varphi(p^m)}{(d, \varphi(p^m))} + \#V_f^{p^{m-d}} \tag{9}$$

for $m > d$ with initial values $\#V_f^{p^m} = \frac{\varphi(p^m)}{(d,\varphi(p^m))} + 1$ for $d \leq m$.

Let $1 \leq k \leq d$ and $k \equiv m \pmod d$. Note that $(d, p^t) = (d, p^{t+d})$ holds when $t \geq d$.

$$\begin{aligned}
\#V_f^{p^m} &= \frac{\varphi(p^m)}{(d,\varphi(p^m))} + \frac{\varphi(p^{m-d})}{(d,\varphi(p^{m-d}))} + \cdots + \frac{\varphi(p^{k+d})}{(d,\varphi(p^{k+d}))} + \frac{\varphi(p^k)}{(d,\varphi(p^k))} + 1 = \\
&= \frac{(p-1)p^{m-1}}{(d,(p-1)p^{m-1})} + \frac{(p-1)p^{m-d-1}}{(d,(p-1)p^{m-d-1})} + \cdots + \frac{(p-1)p^{k-1}}{(d,(p-1)p^{k-1})} + 1 = \\
&= \frac{(p-1)}{(d,(p-1)p^{k+d-1})}\left(p^{m-1} + p^{m-d-1} + \cdots + p^{k+d-1}\right) + \frac{(p-1)p^{k-1}}{(d,(p-1)p^{k-1})} + 1.
\end{aligned} \tag{10}$$

Easily to see that sum $\left(p^{m-1} + p^{m-d-1} + \cdots + p^{k+d-1}\right)$ has $\left\lfloor \frac{m}{d} \right\rfloor$ elements if $d \nmid m$ and $\left\lfloor \frac{m}{d} \right\rfloor - 1$ if $d \mid m$, and in general it can be written as $\left\lfloor \frac{m-1}{d} \right\rfloor$. Then, since the sum is a geometric progression, for that sum with initial value p^{k+d-1} and coefficient p^d, hence:

$$\#V_f^{p^m} = \frac{(p-1)}{(d,(p-1)p^{k+d-1})}\left(p^{k+d-1}\left(\frac{p^{d*\left\lfloor\frac{m-1}{d}\right\rfloor} - 1}{p^d - 1}\right)\right) + \frac{(p-1)p^{k-1}}{(d,(p-1)p^{k-1})} + 1.\blacksquare \tag{11}$$

5.2 Linear polynomials

Consider polynomial $f(x) = ax + b$ over modulo $q = p^m$. Using lemma 8 we assume that $b = 0$. Then two cases are possible:

- if $(a, q) = 1$, then using lemma 8 we have $\#V_f^q = q$

- if $(a,q)=g>1$, then we can divide both modulo and coefficients of f and go to the first case $\#V_f^q=\#V_{f/g}^{q/g}=q/g$

Proposition 10. If $f(x)=ax+b,$ with $a,b\in\mathbb{Z}$ then $\#V_f^q=\frac{q}{(a,q)}$.

5.3 Quadratic polynomials

Consider polynomial $f(x)=ax^2+bx+c$ with integer coefficients over modulo $q=p^m$. Analogously to the case of linear polynomials we assume that $c=0$ and $(a,b,p^m)=1$.

Theorem 11. *Let $f(x)=ax^2+bx\in\mathbb{Z}[x], q=p^m$ then $\#V_f^q$ can be calculated in following way:*

- *if $p=2$*
  - $\#V_f^q=2^m$, *if a is even and b is odd;*
  - $\#V_f^q=2^{m-1}$, *if both a and b are odd;*
  - $\#V_f^q=\left\lfloor\frac{2^m}{6}\right\rfloor+2$, *if a is odd and b is even;*
- *if $p\geq 3$*
  - $\#V_f^q=p^m$, *if a is divided by p;*
  - $\#V_f^q=\left\lfloor\frac{p^{m+1}}{2(p+1)}\right\rfloor+1$ *otherwise;*

□ Let $q=p^m$ with arbitrary prime p.

Consider case, when $a\equiv 0\pmod p$. Show that all values of $f(x)$ for $x=0,1,\ldots,p^m-1$ are distinct. Suppose a contrary, let there exist such u and v, that $f(u)\equiv f(v)\pmod q$ and $u\not\equiv v\pmod q$. Then

$$au^2+bu\equiv av^2+bv\pmod{p^m}\iff a(u+v)(u-v)\equiv -b(u-v)\pmod{p^m}\quad(12)$$

Right part of the congruence isn't congruent to 0. And as a is divided by p, p divides left part in greater power then the right one. Hence they can't be equal and all values of $f(x)$ are distinct and therefore $\#V_f^q=p^m$. This proves cases $p\geq 3$, with a divided by p and $p=2$, with even a and odd b.

In the next part let $p=2$.

Suppose, that both a and b are odd. Note that for both odd and even x $f(x)$ is always even, so $V_f^q\leq 2^{m-1}$. Show that all values of $f(x)$ for odd $x=1,\ldots,2^{m-1}$ are distinct. Suppose a contrary, let there exist such odd u and v, that $f(u)\equiv f(v)\pmod q$ and $u\not\equiv v\pmod q$. Then

$$a(u+v)(u-v)\equiv -b(u-v)\pmod{2^m}\quad(13)$$

And as left part of the congruence is not zero and $u+v\equiv 0 \pmod 2$ and $a,b\not\equiv 0 \pmod 2, 2$ divides right part in greater power. So they can't be equal and all values of $f(x)$ for odd x are distinct and then $\#V_f^q = 2^{m-1}$

Let a be odd and b be even. Then there exists element a^{-1} and $b=2b'$ and we can rewrite f in the following way: $f(x)=ax^2+bx=ax^2+2b'x+a^{-1}b'^2-a^{-1}b'^2=a\big(x^2+2a^{-1}b'x+a^{-2}b'^2\big)-a^{-1}b'^2=a(x+a^{-1}b')^2-a^{-1}b'^2$. And from lemma 8 and corollary 8.1 $\#V_f^q=\#V_{x^2}^q$.

Consider congruence $z^2\equiv t \pmod{2^m}$. It's well known that odd residue is quadratic residue over 2^m if and only if it's of form $8k+1$ [1, chapter 22]. And in case of even $t=2k$, we have $z^2\equiv 2k \pmod{2^m} \iff 4(z')^2\equiv 2k \pmod{2^m} \iff z'^2\equiv k' \pmod{2^{m-2}}$ for some z', k'.

Therefore we can calculate $V_{x^2}^{2^m}$ recursively in the following way:

$$V_{x^2}^{2^m}=\frac{2^m}{8}+V_{x^2}^{2^{m-2}}=2^{m-3}+V_{x^2}^{2^{m-2}} \tag{14}$$

with initial values $V_{x^2}^{2^1}=2$, $V_{x^2}^{2^2}=2$ and $V_{x^2}^{2^3}=3$.

So for odd m:

$$\begin{aligned} V_{x^2}^{2^m} &= 2^{m-3}+2^{m-5}+\cdots+2^2+f(3)= \\ &= 2^{m-3}+2^{m-5}+\cdots+2^2+2^0+2= \\ =\frac{4^{\frac{m-1}{2}}-1}{4-1}+2&=\frac{2^{m-1}-1}{3}+2=\frac{2^m-2}{6}+2=\left\lfloor\frac{2^m}{6}\right\rfloor+2 \end{aligned} \tag{15}$$

And analogously for even m:

$$\begin{aligned} V_{x^2}^{2^m} &= 2^{m-3}+2^{m-5}+\cdots+2^1+f(2)= \\ =2\frac{4^{\frac{m-2}{2}}-1}{4-1}+2&=\frac{2^{m-1}-2}{3}+2=\frac{2^m-4}{6}+2=\left\lfloor\frac{2^m}{6}\right\rfloor+2 \end{aligned} \tag{16}$$

Now let $q=p^m$, with $q\geq 3$.

As $(2,p^m)=(a,p^m)=1$ there exist elements $2^{-1},a^{-1}$. So we can rewrite f as complete square:

$$ax^2+bx=ax^2+bx+2^{-2}a^{-1}b^2-2^{-2}a^{-1}b^2=a\big(x+2^{-1}a^{-1}b\big)^2-2^{-2}a^{-1}b^2 \tag{17}$$

From lemma 8 and corollary 8.1 $V_f^q=V_{x^2}^q$.

Using the formula from theorem 9, with $d=2$, we have

$$\#V_{x^2}^{p^m}=\frac{(p-1)}{(2,(p-1)p^{k+2-1})}\left(p^{k+2-1}\left(\frac{p^{2*\lfloor\frac{m-1}{2}\rfloor}-1}{p^2-1}\right)\right)+\frac{(p-1)p^{k-1}}{(2,(p-1)p^{k-1})}+1.$$

Note that $(2,(p-1)p^{k+2-1})=2$. Since $k\equiv m \pmod d$ and $1\leq k\leq 2$, two different cases are possible.

Odd m and $k=1$:

$$\begin{gathered}
\#V_{x^2}^{p^m} = \frac{(p-1)}{2}\left(p^2\left(\frac{p^{2*\left\lfloor\frac{m-1}{2}\right\rfloor}-1}{p^2-1}\right)\right)+\frac{(p-1)}{2}+1= \\
\frac{(p-1)}{2}\left(p^2\left(\frac{p^{m-1}-1}{p^2-1}\right)+1\right)+1=\frac{(p-1)}{2}\left(\frac{p^{m+1}-p^2+p^2-1}{p^2-1}\right)+1= \qquad (18) \\
\left(\frac{p^{m+1}-1}{2(p+1)}\right)+1=\left\lfloor\frac{p^{m+1}}{2(p+1)}\right\rfloor+1
\end{gathered}$$

Even m and $k=2$:

$$\begin{gathered}
\#V_{x^2}^{p^m} = \frac{(p-1)}{2}\left(p^3\left(\frac{p^{2*\left\lfloor\frac{m-1}{2}\right\rfloor}-1}{p^2-1}\right)\right)+\frac{(p-1)p}{2}+1= \qquad (19) \\
\frac{(p-1)}{2}\left(\frac{p^{m+1}-p^3+p^3-p}{p^2-1}\right)+1=\left(\frac{p^{m+1}-p}{2(p+1)}\right)+1=\left\lfloor\frac{p^{m+1}}{2(p+1)}\right\rfloor+1.\blacksquare
\end{gathered}$$

Corollary 11.1. Using theorems 3 and 11, we can compute the value set of triangular numbers in the following way:

$$V^{2^m}_{\frac{x(x+1)}{2}} = V^{2^{m+1}}_{x^2+x} = 2^m \qquad (20)$$

$$V^{p^m}_{\frac{x(x+1)}{2}} = V^{2*p^m}_{x^2+x} = V^{2}_{x^2+x} * V^{p^m}_{x^2+x} = \left\lfloor\frac{p^{m+1}}{2(p+1)}\right\rfloor+1.$$

6 Generalizations

6.1 Rational functions

We are interested in the problem of calculating the value set of arbitrary integer-valued rational function. It turned out that any such function is in fact an integer-valued polynomial.

Definition 4. We say that a polynomial $g(x)\in\mathbb{R}[x]$ is *almost integer-valued*, if $\forall\varepsilon>0\ \exists n_\varepsilon:\ \forall n>n_\varepsilon\ \exists M_n\in\mathbb{Z}:\ |g(n)-M_n|\le\varepsilon$.

Lemma 12.1 *Let $g(x)\in\mathbb{R}[x]$ be almost integer-valued, then $g(x)$ is integer-valued.*

□ By induction on degree d show that any almost integer-valued polynomial of degree d is integer-valued. For $d=0$ we have that $g(x)$ is constant and hence it's an integer.

Suppose the statement of the induction holds for $d-1$, prove it for d. Consider an arbitrary almost integer-valued polynomial $g(x)$ of degree d, and the polynomial $\triangle g(x) = g(x+1) - g(x)$. We get $g(x) = \sum_{i=0}^{d} t_i \binom{x}{i}$, where t_i are real, so we have:

$$\triangle g(x) = g(x+1) - g(x) = \sum_{i=0}^{d} t_i \left(\binom{x+1}{i} - \binom{x}{i} \right) =$$

$$\sum_{i=0}^{d} \frac{t_i}{i!} \left((x+1)x \dots (x+1-i+1) - x(x-1) \dots (x+1-i) \right) = \tag{21}$$

$$\sum_{i=0}^{d} \frac{t_i}{i!} \left(ix(x-1) \dots (x-i+2) \right) = \sum_{i=1}^{d} t_i \binom{x}{i-1}.$$

Let's prove that polynomial $\triangle g(x)$ is almost integer-valued. Choose arbitrary $\varepsilon > 0$, then $\exists\, n_\varepsilon :\ \forall\, n \geq n_\varepsilon\ \exists M_n :\ |g(n) - M_n| \leq \varepsilon/2$. Hence $\forall n \geq n_\varepsilon$ we have

$$|\triangle g(n) - (M_{n+1} - M_n)| \leq |g(n+1) - M_{n+1}| + |g(n) - M_n| \leq \varepsilon/2 + \varepsilon/2 = \varepsilon.$$

Consequently $\triangle g(x)$ is almost integer-valued, and then by induction it's integer-valued. So by theorem 1 $t_k, \dots t_1$ are integers. Suppose t_0 is not integer. Since $g(x) - t_0$ is an integer-valued polynomial, so $g(x)$ is not almost integer-valued. Hence $t_0 \in \mathbb{Z}$. ■

Theorem 12.2 *Let $R(x) = \frac{f(x)}{g(x)}$ be a rational function, where $f(x), g(x) \in \mathbb{R}[x]$, taking integer values in integer points. Then $R(x)$ is integer-valued polynomial.*

□ Divide f by g with remainder, will get $R(x) = p_k(x) + r(x)$, where p_k is a polynomial, such that $\deg p_k(x) = k$ and $r(x) \to 0$ when $x \to \infty$. Then $p_k(x)$ is an almost integer-valued polynomial. And from lemma 12.1 we have that $p_k(x)$ is integer-valued.

Show that $r(x) = 0$. Since $p_k(x)$ is integer-valued, so $r(x) \in \mathbb{Z}$ for $x \in \mathbb{Z}$ and $r(x) \to 0$ for $x \to \infty$, we have that $r(x)$ have infinity many zeroes. But a rational function having infinity many zeroes is identically equal to zero. ■

6.2 Linear functions of several variables

Proposition 13. *For a linear function $f(x_1, \dots, x_k) = a_1x_1 + a_2x_2 + \dots + a_kx_k + b$ the following is true*

$$\#V_f^n = \frac{n}{(a_1, a_2, \dots, a_k, n)}.$$

□ It's clear that $\#V_f^n = \#V_g^n$, where $g(x_1, x_2, \dots, x_k) = a_1x_1 + a_2x_2 + \dots + a_kx_k$.

If $(a_1, a_2, \dots, a_k, n) = d > 1$, then from properties of congruences, we have $\#V_f^n = \#V_{f/d}^{n/d}$.

In case $(a_1, a_2, \dots, a_k, n) = 1$ there exists at least one such a_i that $(a_i, n) = 1$. Consider that a_i. Obviously we have $\#V_g^n \geq \#V_{a_ix_i}^n$.

And since $\#V_{a_ix_i}^n = n$ for $(a_i, n) = 1$, we have $n \geq \#V_f^n \geq n \iff \#V_f^n = n$. Thus

$$\#V_f^n = \frac{n}{(a_1, a_2, \dots, a_k, n)}. ■$$

References

[1] [in russian*] A. A. Buhshtab "Number Theory". – Prosveschenie Moscow, 1966. – 385 p.

[2] Diaa S. Eldanaf "Value Sets of Polynomials Modulo a Prime" – UMI 1499153, May 2011, California State University, Long Beach.

[3] [in russian*]Prasolov V. V. "Polynomials" – ISBN 5-94057-077-1, MCCME 2003. – 336 p.

[4] http://www.cs.xu.edu/math/math302/04f/PolyCongruences.pdf

[5] S. Uchiyama "The Number of Distinct Values of a Polynomial with Coefficients in a Finite Field"

[*] We're sorry for russian literature, there are only basic knowledge about congruence, indecies and polynomials