2. A number of Residues

Abstract. In this paper we deal with the number of differnt residues a polynomial can have modulo a number n. First, we look at the triangular polynomial $\frac{x(x+1)}{2}$ and find the number for n being a power of 2 or a power of an odd prime. We then use the Chinese remainder theorem in order to prove the multiplicativity of this number given some conditions which implies that if $n = \prod_{p_i \ prime} {p_i}^{k_i}$, $k_i \in \mathbb{Z}_{\geq 0}, p_1 = 2$ is the prime factorization of n, our final formula will be as follows:

$$u_n = 2^{k_1} \cdot \prod_{p_i \neq 2 \ prime} \frac{\sum_{j=1}^{k_i} (-1)^{(k_i - j)} {p_i}^j + \frac{3}{2} + (-1)^{k_i} \cdot \frac{1}{2}}{2}$$

and have thus solved the problem for all n.

In the last part we then go on by generalizing this result to other polynomials up to degree 2 using our previous result and can then reduce polynomials of degree 3 to the well-studied quadratic diophantine equations.

The methods employed are basic algebraic manipulations and basic number theory.

1. Let $n = 2^q$

We have to investigate the problem for how many s the result of $\frac{s(s+1)}{2}$ is equal. First of all we remark that if n is even, the sequence of residues modulo n is $2n$-periodic as $\frac{(s+2n)(s+2n+1)}{2} \equiv \frac{s(s+1)}{2} + \frac{2n(s+2n+1+s)}{2} \equiv \frac{s(s+1)}{2} + n(2s+2n+1) \equiv \frac{s(s+1)}{2}$ modulo n, whereas, if n is odd, it es even n-periodic as there exists a residue l so that $2 \cdot l \equiv 1$ modulo n.

Hence, as in this case n is even, we have to look at how many different residues there are for the terms if $s \in \{0, 1, ..., 2n-1\}$.

This means we can investigate for which m out of this set it is $\frac{s(s+1)}{2} \equiv \frac{m(m+1)}{2}(n)$

$$\begin{aligned}
\frac{s(s+1)}{2} &\equiv \frac{m(m+1)}{2} && (n)\\
\Leftrightarrow \frac{s(s+1) - m(m+1)}{2} &\equiv 0 && (n)\\
\Leftrightarrow \frac{(s-m)(s+m+1)}{2} &\equiv 0 && (n)\\
\Leftrightarrow (s-m)(s+m+1) &\equiv 0 && (2n)\\
\Leftrightarrow (s-m)(s+m+1) &\equiv 0 && (2^{q+1})
\end{aligned}$$

Since $s - m \equiv s + m \not\equiv s + m + 1$ (2), one of the two factors has to be divisible by at least 2^{q+1}. For the first this is only the case if $s \equiv m(2^{q+1})$. From the second we can get a different solution for m where $m \equiv -(s+1)(2^{q+1})$ which means that $m = 2^{q+1} - s - 1 \neq s$ so for each s there is exactly one more m so that the two residues are equal. As there were $2n$ potential residues, there are in total only n distinct ones if n is a power of two.

$\Longrightarrow u_{2^q} = 2^q$.

2. Let $p \neq 2$ be a prime number. Now let us investigate the value of u_{p^k} for arbitrary $k \in \mathbb{Z}_+$. For $n \in \mathbb{N}$ we know that $\frac{n(n+1)}{2} = \frac{(n+\frac{1}{2})^2-\frac{1}{4}}{2} \equiv \frac{(n+\frac{1}{2})^2}{2} - \frac{1}{8} \mod p^k$, while $\frac{1}{8}$ is a fixed residue $\mod p^k$ and the number of the values of $\frac{(n+\frac{1}{2})^2}{2} \mod p^k$, with n running from 0 to $p^k - 1$, equals the number of residues of the form $\frac{x^2}{2} \mod p^k$ for $x \in \left\{0, ..., p^k - 1\right\}$, which, as p^k and 2 are relatively prime, equals the number of quadratic residues $\mod p^k$. Therefore u_{p^k} equals the number of quadratic residues mod p^k.

Let us now investigate the value of u_p for p being an odd prime. Let $a = x^2, x \in \{1, ..., p-1\}$ be a quadratic residue modulo p. We know that $(p-x)^2 \equiv -x^2 \equiv x^2 \equiv a \mod p$ as well as $x \not\equiv p - x \mod p$, because $x + (p - x) = p$ is odd. Therefore, the number of quadratic residues modulo p that are $\neq 0$ is $\leq \frac{p-1}{2}$. But as $\mathbb{F}_p\left(\{0, ..., p-1\}, +, \cdot\right)$ is a field, the quadratic equation $x^2 = a, x \in \mathbb{F}_p$ has a maximum of two roots. Therefore, there is a minimum of $\frac{p-1}{2}$ quadratic residues $\neq 0$ modulo p, thus there are exactly $\frac{p-1}{2}$ of them. Because $0 = 0^2$ is also a quadratic residue, we now know that $u_p = \frac{p-1}{2} + 1 = \frac{p+1}{2}$.

Now let us use induction in order to prove that for every odd p, k, p prime, the equations $u_{p^k} = 1 + \frac{\left(\sum_{j=0}^{k} (-1)^{(k-j)} p^j\right)}{2}$ and $u_{p^{k+1}} = 1 + p \cdot (u_{p^k} - 1) = 1 + p \cdot \left(\frac{\left(\sum_{j=0}^{k} (-1)^{(k-j)} p^j\right)}{2} \right)$ hold. The base clause for $k = 1$ was done above. The following induction step is left to prove:

Let the assumption be true for all odd positive integers $\leq k$. Then also $u_{p^{k+1}} = 1 + p \cdot (u_{p^k} - 1)$ and $u_{p^{k+2}} = 1 + \frac{\left(\sum_{j=0}^{k+2} (-1)^{((k+2)-j)} p^j\right)}{2}$.

Proof. Let us introduce the following lemma:

Lemma. *Let b be a positive integer not divisible by p^m, $m \in \mathbb{Z}_+$. Then for any $a \in \{0, ..., p-1\}$ $b + ap^m$ is a quadratic residue modulo p^{m+1} if and only if b is a quadratic residue modulo p^m.*

Proof. If $b + ap^m$ is a quadratic residue modulo p^{m+1}, there exists an integer x satisfying $x^2 \equiv b + ap^m \mod p^{m+1}$. As $p^m | p^{m+1}$, $x^2 \equiv b + ap^m \equiv b \mod p^m$, so b must be a quadratic residue modulo p^m.
If b is a quadratic residue modulo p^m, there obviously exists an $\tilde{a} \in \{0, ..., p-1\}$ such that $b + \tilde{a}p^m$ is a quadratic residue modulo p^{m+1}, so there exists an integer x satisfying $x^2 \equiv b + \tilde{a}p^m \mod p^{m+1}$, $x^2 \not\equiv 0 \mod p^m$. It is now enough to prove that for every $a \in \{0, ..., p-1\}$ $x^2 + ap^m$ is a quadratic residue modulo p^{m+1}. Choose i, such that $p^i | x, p^{i+1} \nmid x$. As $x^2 \not\equiv 0 \mod p^m$, we know that $2i < m$. Let $y = \frac{x}{p^i}$. As $p \nmid 2, p \nmid y$, there exists a solution z to the equation $2yz \equiv a \mod p^{m+1}$. We finally observe that $(x + zp^{m-i})^2 = (yp^i + zp^{m-i})^2 = (yp^i)^2 + 2yzp^m + z^2 p^{m+(m-2i)} \equiv x^2 + ap^m \mod p^{m+1}$. □

It follows directly from the lemma that there are exactly $p \cdot (u_{p^m} - 1)$ quadratic residues modulo p^{m+1} that are not divisible by p^m, as 0 is always a quadratic residue.

Now I am going to demonstrate why for odd k the equation $u_{p^{k+1}} = 1 + p \cdot (u_{p^k} - 1) = 1 + p \cdot \left(\frac{\left(\sum_{j=0}^{k} (-1)^{(k-j)} p^j \right)}{2} \right)$ holds. 0 is a quadratic residue modulo p^{k+1}, because $0^2 \equiv 0 \mod p^{k+1}$. All other residues a of the form $a = i \cdot p^k$, $i \in \{1, ..., p-1\}$, are quadratic

nonresidues modulo p^{k+1}, because a product of two factors is a quadratic residue if and only if either both factors are quadratic residues or quadratic nonresidues; in this case $a = i \cdot p^k = a = ip \cdot p^{k-1}$. Obviously p^{k-1} is a quadratic residue, but, as $p \not| i$, ip is a quadratic nonresidue.

Let each residue $a \in \left\{0, ..., p^{k+1} - 1\right\}$ be written of the form $a = ip^k + m$, $i \in \left\{0, ..., p-1\right\}, m \in \left\{0, ..., p^k - 1\right\}$. It can be easily seen that if $\tilde{m}$ is a quadratic nonresidue modulo p^k, all numbers of the form $ip^k + \tilde{m}$ are quadratic nonresidues modulo p^{k+1}. As there are $\frac{\left(\sum_{j=0}^{k} (-1)^{(k-j)} p^j\right)}{2}$ non-zero quadratic residues modulo p^k, there are at most $p \cdot \frac{\left(\sum_{j=0}^{k} (-1)^{(k-j)} p^j\right)}{2}$ non-zero quadratic residues modulo p^{k+1}. From the lemma we know that if m is a non-zero quadratic residue modulo p^k, all residues $ip^k + m$, $i \in \{0, ..., p-1\}$, are quadratic modulo p^{k+1}, such that there is a total of exactly $1 + p \cdot \frac{\left(\sum_{j=0}^{k} (-1)^{(k-j)} p^j\right)}{2}$ quadratic residues modulo p^{k+1}, $\Longrightarrow u_{p^{k+1}} = 1 + p \cdot \frac{\left(\sum_{j=0}^{k} (-1)^{(k-j)} p^j\right)}{2}$.

Now it is still left to prove that $u_{p^{k+2}} = 1 + \frac{\left(\sum_{j=0}^{k+2} (-1)^{((k+2)-j)} p^j\right)}{2}$.

Obviously, 0 is a quadratic residue modulo p^{k+2}. As shown above, there are $p(u_{p^k} - 1)$ non-zero quadratic residues modulo p^{k+1}. Now we can apply the lemma on $m = k+1$. Therefore we know that there are $p \cdot p\left(u_{p^k} - 1\right) = p^2 \cdot \frac{\left(\sum_{j=0}^{k} (-1)^{(k-j)} p^j\right)}{2}$ quadratic

residues modulo p^{k+2} that are not divisible by p^{k+1}. We still need to investigate the number of residues of the form $i \cdot p^{k+1}$, $i \in \{1, ..., p-1\}$. As $i \cdot p^{k+1}$ is a quadratic residue if and only if i is a quadratic residue modulo p^{k+2}, which is the case if and only if i is a quadratic residue modulo p, this number equals $u_p - 1 = \frac{p-1}{2}$. So we now know that there is a total of $u_{p^{k+2}} = 1 + p^2 \cdot \frac{\left(\sum_{j=0}^{k} (-1)^{(k-j)} p^j\right)}{2} + u_p = 1 + \frac{\left(\sum_{j=0}^{k+2} (-1)^{((k+2)-j)} p^j\right)}{2}$ quadratic residues modulo p^{k+2}. □

Therefore it is shown that $u_{p^k} = 1 + \frac{\left(\sum_{j=0}^{k} (-1)^{(k-j)} p^j\right)}{2}$ for odd k and $u_{p^k} = 1 + p \cdot \frac{\left(\sum_{j=0}^{k-1} (-1)^{((k-1)-j)} p^j\right)}{2}$ for even $k > 0$, whenever p is an odd prime. This can be summarized as $u_{p^k} = \frac{\sum_{j=1}^{k} (-1)^{(k-j)} p^j + \frac{3}{2} + (-1)^k \cdot \frac{1}{2}}{2}$ for arbitrary positive integers k.

3. The value of u_n in the general case can be easily deducted from the values of u_{p^k}, p prime, $k \in \mathbb{Z}_+$. Triangular numbers are always n-periodic modulo any odd n, since

$$(n+a)(n+a+1) = n^2 + 2na + a^2 + n + a \equiv a^2 + a \mod n$$
$$\implies \frac{(n+a)(n+a+1)}{2} \equiv \frac{a(a+1)}{2} \mod n$$

. Moreover, triangular numbers are always 2^{m+1}-periodic modulo 2^m, $m \in \mathbb{Z}_{\geq 0}$, because $(2^{m+1}+a)(2^{m+1}+a+1) = 2^{2m+2} + 2^{m+2}a + a^2 + 2^{m+1} + a \equiv a^2 + a \mod 2^{m+1} \implies \frac{(2^{m+1}+a)(2^{m+1}+a+1)}{2} \equiv \frac{a(a+1)}{2} \mod 2^{m+1}$. For any prime p let k be a non-negative integer satisfying $p^k | n, p^{k+1} \not| n$. As triangular numbers are p^k-periodic $\mod p^k$ for odd p as well as $2p^k$-periodic for $p = 2$. Let $n = \prod_{p_i \ prime} {p_i}^{k_i}$, $k_i \in \mathbb{Z}_{\geq 0}$ be the prime factorization of n, w.l.o.g. $p_1 = 2$. Because the lengths of the periods of triangular numbers $\mod p_i^{k_i}$ are relatively prime (see above), it may be concluded by the chinese remainder theorem that it is possible to find a number $m \in \{0, ..., 2n\}$ satisfying $m \equiv m_i \mod p_i^{k_i}$ for every i and for every $m_1 \in \left\{0, ..., 2^{k_1+1} - 1\right\}, m_i \in \left\{0, ..., {p_i}^{k_i} - 1\right\}, i \geq 2$, assuming that m_i is a possible residue of triangular numbers modulo $2^{k_1+1}, i = 1$ and modulo ${p_i}^{k_i}, i \geq 2$, respectively (i.e. modulo the periodic lenghts). Therefore the number of possible residues of triangular numbers modulo n equals the product of the $u_{{p_i}^{k_i}}$, ${p_i}^{k_i} || n$.

Thus for every $n = \prod_{p_i \ prime} {p_i}^{k_i}$, $p_1 = 2, k_i \in \mathbb{Z}_{\geq 0}$ we get the following general formula: $u_n = \prod_{p_i \ prime} u_{{p_i}^{k_i}} = 2^{k_1} \cdot \prod_{p_i \neq 2 \ prime} u_{{p_i}^{k_i}} = 2^{k_1} \cdot \prod_{p_i \neq 2 \ prime} \frac{\sum_{j=1}^{k_i} (-1)^{(k_i - j)} {p_i}^j + \frac{3}{2} + (-1)^{k_i} \cdot \frac{1}{2}}{2}$ (noticing that $u_1 = 1$).

4. Let $u_{P,n}$ denote the number of residues modulo n that a polynomial $P : \mathbb{Z} \longrightarrow \mathbb{Z}$ with rational coefficients could adopt. It is obvious that $u_{(C),n} = 1$ for all $C, n \in \mathbb{Z}$. Also, the constant term of every polynomial needs to be an integer in order to achieve integer values, so from now on we assume that the constant term is integer. Let us now investigate the value of $u_{(ax+C),n}$. It is a well-known fact that ax can adopt an amount of $\frac{n}{gcd(a,n)}$ different residues modulo n, such that, independently of the value of C, $u_{(ax+C),n} = \frac{n}{gcd(a,n)}$.

Now let us consider $P(x) = ax^2 + bx + c$. As we are looking for the number u_p of different non-zero residues modulo an odd prime p we can ignore the constant and after multiplying with a^{-1} we get a polynomial of the form $x(x+b)$. Analogously to **1** we have

$$\begin{aligned} x^2 + bx &\equiv y^2 + by && \mod p \\ (x-y)(x+y+b) &\equiv 0 && \mod p \\ x \equiv y \mod p \vee x &\equiv -y - b \mod p \end{aligned}$$

The first solution is obvious. The second solution is a solution as well as can be seen by simply inserting, so we know that each non-zero residue will be adopted by either 0 or 2 distinct x modulo p. Therefore, analogously to **1**, the polynomial $x(x+b)$ adopts exactly $\frac{p-1}{2}$ non-zero residues modulo p. By inserting $x = 0$, we learn that the residue 0 will also be adopted, so that $u_p = \frac{p+1}{2}$. For $p = 2$, $P(0) \equiv c \mod 2$. If both a and b are even, $ax^2 + bx + c \equiv c \mod 2$, such that $u_2 = 1$, also if both a and b are odd. If exactly one of these two coefficients is odd, we observe that $P(1) = a + b + c \equiv c + 1 \mod 2$, such that $u_2 = 2$. For a prime p relatively prime to the rational coefficients a, b we obtain, analogously to **2**, that u_{p^k} is the number of

quadratic residues modulo p^k, which was calculated above for odd p. Then we can use the Chinese remainder theorem similarly to **3** to calculate the value of u_n.

Having $P(x) = ax^3 + bx^2 + cx + d$ due to Cardano's transformation we can drop the quadratic term. Then we can drop the constant term and multiply with a^{-1} again and thus all cubic polynomials of interest have the form $P(x) = x^3 + cx$. Now what if $P(x) = P(y)$ modulo an odd prime p:

$$\begin{aligned} x^3 + cx &\equiv y^2 + cy && \mod p \\ (x-y)(x^2 + xy + y^2 + c) &\equiv 0 && \mod p \\ x \equiv y \mod p \vee x^2 + xy + y^2 + c &\equiv 0 \mod p \end{aligned}$$

The number u_p is now determined by the number of solutions of the quadratic diophantine equation, for which a solution is known.

References.

www.oemo.at/wiki/images/f/f5/Zahlentheorie_Heuberger.pdf, 29.06.2012