Прибор для ускоренного вычисления степенных вычетов по данному нечетному первоначальному модулю *).

М. Н. Марчевский.

1. Из элементарной теории чисел известно, что целое число A называется ***вычетом*** $m^{\text{-ой}}$ ***степени*** по данному нечетному первоначальному модулю p в том случае, если оказывается возможным сравнение

$$x^m \equiv A \pmod{p}; \quad \ldots\ldots\ldots\ldots (1)$$

если же не существует значений x удовлетворяющих этому сравнению, то число A называется ***невычетом*** $m^{\text{-ой}}$ ***степени*** по модулю p. Относительно сравнений вида (1) существует следующая теорема **).

„Сравнение (1) возможно только в том случае, когда

$$A^{\frac{p-1}{\omega}} \equiv 1 \pmod{p},$$

где ω — общий наибольший делитель чисел $p-1$ и m".

Мы предположим везде в дальнейшем, что $p-1$ делится на m; тогда, очевидно, в предыдущей теореме будет $\omega = m$, и все вычеты A по модулю p найдутся из сравнения

$$A^{\frac{p-1}{m}} \equiv 1 \pmod{p} \quad \ldots\ldots\ldots\ldots (2)$$

Чтобы ответить на вопрос, сколько существует ***различных*** (т.-е. не сравнимых по модулю p) вычетов $m^{\text{-ой}}$ степени по нечетному первоначальному модулю p, припомним еще одну теорему из теории чисел, а именно ***):

„Сравнение $x^n - 1 \equiv 0 \pmod{p}$ имеет d решений, где d есть общий наибольший делитель чисел n и $p-1$".

Обращаясь к сравнению (2), мы видим, что общий наибольший делитель d чисел $n = \frac{p-1}{m}$ и $p-1$ есть $d = \frac{p-1}{m}$, следовательно,

---

*) Прибор этот демонстрировался в заседаниях научно-исследовательской кафедры математического анализа 20.I.27 и Харьковского Математического Общества 24.II.27.

**) См., напр., *Чебышев*, Теория сравнений, изд. 3-е 1901 г., стр. 100 (в теореме предполагается, что A не делится на p).

***) *Чебышев*, ibid. стр. 96.

сравнение (2) даст $\frac{p-1}{m}$ различных значений для A, а потому мы заключаем, что:

Число различных вычетов m-ой степени по нечетному первоначальному модулю p равно $\frac{p-1}{m}$, при условии, что $p-1$ делится на m.

Так, например, по модулю $p=13$ существует 6 квадратичных вычетов (а именно: 1, 3, 4, 9, 10, 12), 4 кубических вычета (1, 5, 8, 12) и 2 вычета 6-ой степени (1 и 12).

2. Условимся (в соответствии с немецкими словами „Rest" — вычет и „Nichtrest" — невычет) обозначать различные вычеты буквами $R, R_1 R_2 \ldots$, а невычеты — буквами $N, N_1 N_2, \ldots$ Тогда в случае *квадратичных* вычетов по нечетному первоначальному модулю имеем хорошо известные свойства:

1. ***Произведение двух вычетов есть также вычет*** (т.-е. $R_1 . R_2 = R$)
2. ***Произведение вычета на невычет есть невычет*** (т.-е. $R_1 . N_1 = N$)
3. ***Произведение двух невычетов есть вычет*** (т.-е. $N_1 . N_2 = R$)

Легко показать, что для вычетов любой степени по нечетному первоначальному модулю сохранят силу лишь первые два свойства, третье же может и не иметь места, иначе говоря, произведение двух невычетов может в одних случаях дать вычет, а в других — остаться невычетом.

Действительно, если R_1 и R_2 — вычеты, то по (2) имеем

$$R_1^{\frac{p-1}{m}} \equiv 1 \pmod{p}, \quad R_2^{\frac{p-1}{m}} \equiv 1 \pmod{p};$$

перемножая эти сравнения, имеем

$$(R_1 R_2)^{\frac{p-1}{m}} \equiv 1 \pmod{p},$$

откуда и вытекает свойство 1^0. Если далее R_1 — вычет, а N_1 — невычет, то тогда

$$R_1^{\frac{p-1}{m}} \equiv 1 \pmod{p}, \quad N_1^{\frac{p-1}{m}} \equiv k \pmod{p}, \quad \text{где } k \neq 1;$$

отсюда получается свойство 2^0, так как теперь

$$(R_1 . N_1)^{\frac{p-1}{m}} \equiv k \pmod{p} \text{ и } k \neq 1.$$

Наконец, если N_1 и N_2 — невычеты, то из сравнений

$$N_1^{\frac{p-1}{m}} \equiv k_1 \pmod{p}, \quad N_2^{\frac{p-1}{m}} \equiv k_2 \pmod{p}, \quad \text{где } k_1 \neq 1 \text{ и } k_2 \neq 1,$$

вытекает лишь то, что

$$(N_1 . N_2)^{\frac{p-1}{m}} \equiv k_1 . k_2 \pmod{p},$$

и тогда возможны случаи как

$$k_1 . k_2 \equiv 1 \pmod{p}, \text{ так и } k_1 . k_2 \equiv k \pmod{p}, \text{ где } k \neq 1;$$

в первом случае произведение $N_1 . N_2$ окажется вычетом, во втором — невычетом.

3. Заметим еще, что *всякое целое число, равное m-ой степени другого целого числа, является вычетом m-ой степени по модулю p,* потому что, если $R = k^m$, то сравнение

$$x^m \equiv R \pmod{p}$$

имеет очевидное решение $x = k$.

На основании этого соображения можно практически находить степенные вычеты. Так, например, выше было упомянуто, что при $p = 13$ существует 6 квадратичных вычетов, а именно, числа 1, 3, 4, 9, 10, 12. Их можно было бы найти, пользуясь тем, что все точные квадраты должны быть квадратичными вычетами. Написав первые 6 квадратов: 1, 4, 9, 16, 25, 36 и заменив последние 3 числа числами 3, 12, 10 (сравнимыми с ними по модулю 13) мы и получим упомянутые 6 вычетов лишь в ином порядке.

Иногда, впрочем, такой способ может оказаться и неудобным. Например, чтобы найти для того же модуля $p = 13$ все 4 кубических вычета: 1, 5, 8, 12, станем выписывать точные кубы; тогда мы увидим, что

$$1^3 = 1,\ 2^3 = 8,\ (3^3 = 27 \equiv 1),\ 4^3 = 64 \equiv 12,\ (5^3 = 125 \equiv 8),$$
$$(6^3 = 216 \equiv 8),\ 7^3 = 343 \equiv 5;$$

таким образом, пришлось сделать три лишних вычисления, поставленные нами в скобках, пока не получились все требуемые кубические вычеты.

4. Из предыдущего ясно, насколько желательны всякие упрощения в процессе вычисления степенных вычетов. Мы ограничимся следующими указаниями ($1^0 — 7^0$):

1^0. Число 2 есть квадратичный вычет простых чисел вида $p = 8k + 1$ и $p = 8k + 7$ и квадратичный невычет простых чисел вида $p = 8k + 3$ и $p = 8k + 5$ *).

2^0. Для простых чисел вида $p = 4k + 1$ два числа a и $p — a$ являются или оба квадратичными вычетами или оба квадратичными невычетами **).

3^0. Для простых чисел вида $p = 4k + 3$ одно из двух чисел a и $p — a$ является квадратичным вычетом, а другое квадратичным невычетом **).

Следующие свойства $4^0 — 7^0$ относятся к любому нечетному простому модулю.

4^0. Два числа a и $p — a$ являются или одновременно вычетами или одновременно невычетами *нечетной* степени.

Для доказательства положим, что a есть вычет нечетной степени по модулю p, т.-е. что имеет место сравнение

*) См. напр., *Gauss*, Disquisitiones arithmeticae, §§ 112 — 114 (Werke, Bd. I. стр. 84 — 86).

**) Ibid., § 111 (стр. 84).

$$x^{2m+1} \equiv a \pmod{p};$$

тогда, очевидно, можно написать:

$$-x^{2m+1} \equiv -a \pmod{p}, \quad (-x)^{2m+1} \equiv p-a \pmod{p},$$

откуда и видно, что $p-a$ тоже есть вычет. Если бы a было невычетом нечетной степени, то и $p-a$ тоже оказалось бы невычетом, ибо иначе, в силу только что доказанного, число $p-(p-a)=a$ было бы вычетом, что противоречит допущению.

5°. Если два вычета R_1 и R_2 одной и той же степени таковы, что R_1 делится на R_2, то частное $R_1 : R_2$ также будет вычетом.

Действительно, предположение $R_1 : R_2 = N$ невозможно, потому что тогда мы имели бы $R_2 N = R_1$, тогда как $R_2 N$ должно быть невычетом.

6°. Для вычетов и невычетов одной и той же степени, в случае делимости вычета на невычет или невычета на вычет, частное всегда будет невычетом.

Это, подобно предыдущему, видно из невозможности предположений, что $R_1 : N_1 = R$ или $N_1 : R_1 = R$, откуда и вытекает, что $R_1 : N_1 = N$ и $N_1 : R_1 = N$.

7°. В случае делимости друг на друга двух ***квадратичных*** невычетов, их частное $N_1 : N_2$ будет вычетом.

Это видно из невозможности для ***квадратичных*** невычетов допущения $N_1 : N_2 = N$, из которого следовало бы $N_2 N = N_1$, тогда как $N_2 N$ есть квадратичный вычет.

5. После всего сказанного мы уже можем перейти к выяснению очень простой идеи, положенной в основу конструкции прибора, часто позволяющего очень легко и быстро вычислить все вычеты по данному нечетному простому модулю p.

Условимся для краткости называть числа a и $p-a$ (где $a<p$) ***дополнительными*** одно для другого, и представим себе, что числа $1, 2, 3, \ldots p-3, p-2, p-1$ написаны в две строки так, что в верхней находится первая половина числа $\left(\text{от } 1 \text{ до } \frac{p-1}{2}\right)$ а в нижней — все остальные числа ***в обратном порядке*** $\left(\text{от } \frac{p+1}{2} \text{ до } p-1, \text{ идя } \textit{справа налево}\right)$:

$$\left.\begin{array}{llll} 1, & 2, & 3, & \ldots\ldots \dfrac{p-1}{2} \\ p-1, & p-2, & p-3, & \ldots\ldots \dfrac{p+1}{2} \end{array}\right\} \quad \ldots\ldots (3)$$

При таком расположении мы видим, что в каждом вертикальном столбце в (3) располагаются числа дополнительные друг другу. Так, для модуля $p=13$ мы получили бы следующие две строки чисел:

$$\left.\begin{array}{llllll} 1, & 2, & 3, & 4, & 5, & 6 \\ 12, & 11, & 10, & 9, & 8, & 7 \end{array}\right\} \quad \ldots\ldots\ldots\ldots (4)$$

Воспользуемся этим примером для того, чтобы показать упрощенный способ вычисления, например, *кубических* вычетов по модулю 13, число которых, как мы знаем, должно быть равно $4\left(=\frac{13-1}{3}\right)$. К числу этих вычетов должны принадлежать 1 и 8, как точные кубы. Остальные же два вычета найдутся на основании указания 4°, при чем, благодаря сделанному расположению чисел (4) в две строчки, эти вычеты $13-1=12$ и $13-8=5$ окажутся в тех же вертикальных рядах, в которых находятся два предыдущих вычета 1 и 8. Чтобы отметить это обстоятельство, мы поставили одну точку между числами 1 и 12, а другую — между 8 и 5. Такого рода точки, поставленные *между* двумя числами одного вертикального ряда, будут всегда означать, что *оба* эти числа одновременно являются вычетами.

Остается посмотреть, как отмечать вычеты в тех случаях, когда при наличности двух строчек типа (3) из двух чисел одного вертикального ряда одно будет вычетом, а другое — невычетом, как это, например, бывает при нахождении квадратичных вычетов по модулю $p=4k+3$ (см. указание 3°).

Мы условимся в тех случаях когда вычет находится в *верхней* строчке, ставить точку *над* ним, когда же он находится в *нижней* строчке, ставить точку *под* ним.

Положим для примера, что мы ищем все квадратичные вычеты по модулю $p=11$ (типа $4k+3$). Тогда очень легко прийдем к следующей схеме:

$$\begin{matrix} \overset{\bullet}{1} & 2 & \overset{\bullet}{3} & \overset{\bullet}{4} & \overset{\bullet}{5} \\ 10 & \underset{\bullet}{9} & 8 & 7 & 6 \end{matrix}$$

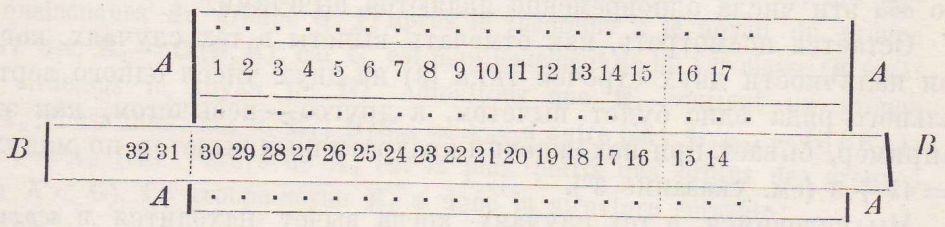
Действительно, отмечаем прежде всего числа 1, 4, 9, как точные квадраты; тогда *дополнительные* для них числа 10, 7, 2 представят, по 3°, невычеты. Частное $10:2=5$ от деления двух невычетов даст, по 7°, вычет, следовательно, 6 будет невычетом. Наконец, частное $6:2=3$ от деления двух невычетов снова даст вычет. Отсюда и получатся все $5\left(=\frac{11-1}{2}\right)$ квадратичных вычетов по модулю 11, отмеченные точками.

Вычисление вычетов можно, разумеется, производить различными способами. Например, в последнем примере вместо того, чтобы отыскивать вычет 5 путем деления 10:2, можно было бы воспользоваться тем, что число 16 (не содержащееся в нашей схеме), как точный квадрат, является квадратичным вычетом; отняв от него модуль, т.-е. 11, снова получим в качестве вычета число 5. Делая те или иные изменения в процессе вычисления вычетов, нужно лишь заботиться об упрощении выкладок. Дать здесь какие-либо специальные правила не представляется возможным; каждый может действовать так, как ему представляется удобней.

6. Из разобранных примеров видно, что в каждом отдельном случае нужно особо выписывать две строчки, и что числа, отмеченные в одном случае, как вычеты, в другом случае могут оказаться невычетами.

Можно однако построить такой прибор, который позволял бы производить вычисления вычетов по различным модулям, ничего каждый раз не выписывая и не делая никаких *письменных* отметок (которые, будучи пригодны в одном случае, могли бы в другом оказаться совершенно неприменимыми).

Представим себе две линейки (см. чертеж) одну A — неподвижную, а другую B — подвижную, которая могла бы скользить вдоль первой (на подобие движка логарифмической линейки).



На неподвижной линейке A написаны натуральные числа 1, 2, 3, 4.... в нормальном порядке, а на подвижной B (будем называть ее *движком*) — те же числа в обратном порядке. Кроме того, на линейке A сделаны три ряда отверстий, отмеченных на чертеже точками. Верхний ряд отверстий приходится над числами линейки A, средний ряд — под теми же числами (между числами линейки и движка), наконец, нижний ряд — под числами движка. Установка движка производится так, чтобы образовались две строки чисел типа (3) № 5. Остальные числа движка и линейки оказываются излишними для рассматриваемого частного случая, и на них не нужно обращать никакого внимания. На чертеже указана установка для модуля $p = 31$; пунктиром отмечены границы слева и справа, между которыми заключаются все необходимые для данного случая числа.

Самая отметка чисел производится путем втыкания штифтов в соответствующие отверстия упомянутых рядов. Когда требуемое число штифтов правильно установлено на линейке, мы можем прямо на ней и на движке прочесть все вычеты по взятому модулю. Записав результат, можем вынуть все штифты, и прибор снова может быть применен (после новой установки движка) для вычисления вычетов по какому-нибудь другому модулю.

Для иллюстрации быстроты таких вычислений, положим, что для модуля $p = 157$ требуется найти все *кубические* вычеты, число которых равно $52 \left(= \frac{157-1}{3}\right)$. Установив движок так, чтобы на линейке стояли числа от 1 до 78, а на движке — от 79 до 156 в обратном порядке мы должны (по указанию 4^0) найти все 52 вычета в 26 вертикальных рядах, т.-е. на приборе нужно будет вставить 26 штифтов

в *среднем* ряду. По окончании вычислений все 52 кубических вычета по модулю 157 будут следующие:

1	2	4	7	**8**	14	16	23	**27**	28	29	32	39
156	155	153	150	149	143	141	134	130	129	128	**125**	118
41	45	46	49	54	56	58	59	**64**	65	67	75	78
116	112	111	108	103	101	99	98	93	92	90	82	79

Самое же вычисление вычетов можно быстро произвести, например, так. Отметив прежде всего точные кубы: 1, 8, 27 64 и 125, мы уже получаем 5 пар кубических вычетов. Заметив, что в числе их оказалось число 32 (в одном столбце с 125), можем получать дальнейшие вычеты так:

1) $64:32=2$ (и 155); 2) $2.27=54$ (и 103); 3) $2.54=108$ (и 49); 4) $2.49=98$ (и 59); 5) $2.59=118$ (и 39); 6) $2.39=78$ (и 79); 7) $2.64=128$ (и 29); 8) $2.29=58$ (и 99); 9) $2.58=116$ (и 41); 10) $2.41=82$ (и 75); 11) $2.75=150$ (и 7); 12) $2.7=14$ (и 143); 13) $2.14=28$ (и 129); 14) $2.28=56$ (и 101); 15) $2.56=112$ (и 45); 16) $2.45=90$ (и 67); 17) $2.67=134$ (и 23); 18) $2.23=46$ (и 111); 19) $2.46=92$ (и 65); 20) $2.2=4$ (и 153); 21) $2.8=16$ (и 141).

Присоединяя эту 21 пару вычетов к ранее указанным 5 парам, мы и получим все 52 кубических вычета по модулю 157. Так как все только что приведенные вычисления совершаются очень быстро в уме, то ясно, что все 26 штифтов будут в течение очень короткого промежутка времени расставлены в надлежащих местах, и нам останется лишь записать окончательный результат.

M. Marczewsky. Appareil pour l'évaluation rapide des résidus pour un module premier impair. Resumé. Profitant les propriétés élémentaires des résidus et des non-résidus (№ 4, $1^0 - 7^0$) je construisis un appareil pour l'évaluation rapide des résidus. Il se compose de même que la règle logarithmique de deux parties A et B dont la première est immobile et la deuxième au contraire mobile (voir la figure dans № 6). La partie A contient trois rangées d'ouvertures pour y placer des goupilles, qui servent à noter des résidus à l'aide des remarques signalées plus haut (№ 4, $1^0 - 7^0$). Quand les deux règles A et B sont placées d'une manière convenable et tous les résidus sont marqués par des goupilles, on doit seulement inscrire le résultat, et puis on peut retirer les goupilles et l'appareil est prêt pour les nouvelles évaluations des résidus pour un autre module quelconque.