ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 33, Number 4, Winter 2003

COUNTING THE NUMBER OF SOLUTIONS OF LINEAR CONGRUENCES

G. SBURLATI

ABSTRACT. We analyze some known formulas which concern counting the number of solutions of linear congruences and we find two important related numerical values which give an answer to interesting questions in elementary number theory related to distributions of sums modulo an integer. Two different ways to obtain good approximations of such values are discussed.

1. Introduction. Starting from known formulas giving the number of solutions of linear congruences with conditions on the greatest common divisor of each variable, in this paper a number of mathematical properties are derived which give an answer to questions like these: a finite set E of prime numbers being fixed, what are the integers favored as possible results of a sum having, for each prime p lying in E, a given number of addenda which are not multiples of p? If one also fixes a number $v \in \mathbf{N}$, how much can each single integer $m \in \mathbf{N}$ be favored or not favored if, for each p, in the sum there are at least v addenda not multiples of p? To answer the second question, we analyze from a qualitative and quantitative point of view two important values depending on v and related to linear congruences and, by proving two theorems and properties, we obtain their numerical expressions and two possible ways to calculate good approximations of them.

2. Some known results on linear congruences. We consider the problem of finding the elements $(x_1, x_2, \dots, x_k) \in \mathbf{Z}_r^k$ which satisfy the congruence equation

$$\sum_{j=1}^{k} h_j x_j \equiv a \pmod{r}, \tag{1}$$

and the constraining equalities

$$(x_j, r) = d_j; \quad j = 1, 2, \dots, k, \tag{2}$$

Received by the editors on March 26, 2001.

where r and k are fixed positive integers, $h_1, h_2, \dots, h_k$ and a are fixed residual classes in $\mathbf{Z}_r$ and $d_1, d_2, \dots, d_k$ are k divisors, not necessarily distinct, of r. (Compare this problem with the problems treated in [**1**].)

Formulas are presently known which give the total number of solutions of (1) and (2) (we remark that these formulas, however, are not constructive, i.e., they do not allow explicitly finding such solutions). Calling N_a the number of solutions, it is known for example that, when $h_1 \equiv h_2 \equiv \cdots \equiv h_k \equiv 1 \pmod{r}$, the following equality is satisfied:

$$N_a = \frac{1}{r} \sum_{d|r} c\left(\frac{r}{d}; \frac{r}{d_1}\right) c\left(\frac{r}{d}; \frac{r}{d_2}\right) \cdots c\left(\frac{r}{d}; \frac{r}{d_k}\right) c(a; d), \tag{3}$$

where, for all $m, n \in \mathbf{N}$, $c(m; n)$ is the integer $\sum_{j=1,\ (j;n)=1}^{n} (e^{2\pi i/n})^{jm}$ (see [**2**, p. 138]).

Let us pose, for each prime divisor p of r, $b_p = \sharp(\{j, 1 \le j \le k : p \nmid h_j d_j\})$ and let us assume that, for each $p, b_p \ge 1$.

We now pose, for each j with $1 \le j \le k$, $g_j = (h_j d_j, r)$ and we apply formula (3) to the problem given by equation $\sum_{j=1}^{k} y_j \equiv a \pmod{r}$ and by constraints $(y_j, r) = g_j$ for $j = 1, 2, \dots, k$. Then in the expression obtained for N_a we replace the $c(m; n)$ by their values as given by Hölder's equalities (for all $m, n \in \mathbf{N}$, $c(m; n) = (\varphi(n)/\varphi(n/(n; m))) \cdot \mu(n/(n; m))$, φ and μ being, respectively, Euler's and Moëbius' functions, see [**3**]). Successively we multiply the obtained value of N_a by the integer

$$\nu = \frac{\varphi(r/d_1)}{\varphi(r/g_1)} \cdot \frac{\varphi(r/d_2)}{\varphi(r/g_2)} \cdots \frac{\varphi(r/d_k)}{\varphi(r/g_k)},$$

which is the ratio of the number of $(x_1, x_2, \dots, x_k) \in \mathbf{Z}_r^k$ satisfying constraints (2) to the number of $(y_1, y_2, \dots, y_k) \in \mathbf{Z}_r^k$ satisfying constraints $(y_j, r) = g_j$ for $j = 1, 2, \dots, k$. νN_a is the number of solutions of (1) and (2). Finally we manipulate the expression of such a number by using basic properties of functions φ and μ and by applying, proceeding in reverse order, the distributive property of the product with respect to the sum. We obtain instead of (3) the following equality, holding for generic $h_1, h_2, \dots, h_k$:

$$N_a = \frac{\varphi(r/d_1)\varphi(r/d_2) \cdots \varphi(r/d_k)}{r} \cdot P_a, \tag{4}$$

where

$$P_a = \prod_{\substack{p\mid r\\ p\nmid a}} \left[1 - \frac{(-1)^{b_p}}{(p-1)^{b_p}}\right] \cdot \prod_{\substack{p\mid r\\ p\mid a}} \left[1 - \frac{(-1)^{b_p-1}}{(p-1)^{b_p-1}}\right]. \tag{5}$$

The latter formula, in the particular case $h_1 \equiv h_2 \equiv \cdots \equiv h_k \equiv 1 \pmod r$ and $d_1 = d_2 = \cdots = d_k = 1$ can be found in [**3**]. Compare equalities (4) and (5) also with [**4**].

From (4) and (5) we deduce that, varying only the class a in the problem given by (1) and (2), the number N_a depends only on the value $(a; r)$. Then for each divisor d of r, denoting by $N_{\gcd=d}$ the number of $(x_1; x_2; \ldots; x_k) \in \mathbf{Z}_r^k$ satisfying (2) such that $(\sum_{j=1}^k h_j x_j, r) = d$, we can write $N_{\gcd=d} = \varphi(r/d) \cdot N_a$, where a is any element of $\mathbf{Z}_r$ such that $(a; r) = d$.

The following example may help to clarify the procedure. Let us consider the problem given by the following equation and constraints:

$$x_1 + x_2 + x_3 \equiv a \pmod{105};$$
$$(x_1, 105) = 1, (x_2, 105) = 5, \quad (x_3, 105) = 7.$$

From the above definitions, we have $r = 105$, $d_1 = 1$, $d_2 = 5$, $d_3 = 7$, $b_3 = 3$, $b_5 = b_7 = 2$. Then from (4) we obtain, for each $a \in \mathbf{Z}_{105}$,

$$N_a = \frac{\varphi(105)\varphi(21)\varphi(15)}{105} \cdot P_a = \frac{48 \cdot 12 \cdot 8}{105} \cdot P_a = \frac{1536}{35} \cdot P_a.$$

The Table (following page) shows the values of P_a, N_a and $N_{\gcd=(a,105)}$ corresponding to each value of $(a, 105)$.

We can notice that the values of P_a corresponding to the eight divisors of 105 are the results of the eight possible products in which the first factor is either 9/8 or 3/4, the second factor is either 15/16 or 5/4 and the third factor is either 35/36 or 7/6.

3. Qualitative analysis of the above results. $\varphi(r/d_1)\varphi(r/d_2) \ldots \varphi(r/d_k)$ is the number of the elements in $\mathbf{Z}_r^k(x_1, x_2, \ldots, x_k)$ which satisfy constraints (2). If we keep the left-hand side of equation (1) and conditions (2) fixed and we vary a in $\mathbf{Z}_r$, it is clear that the arithmetic

$(a, 105)$	P_a	N_a	$N_{\gcd=(a,105)}$
1	$\frac{9}{8}\cdot\frac{15}{16}\cdot\frac{35}{36}=\frac{525}{512}$	45	2160
3	$\frac{3}{4}\cdot\frac{15}{16}\cdot\frac{35}{36}=\frac{175}{256}$	30	720
5	$\frac{9}{8}\cdot\frac{5}{4}\cdot\frac{35}{36}=\frac{175}{128}$	60	720
7	$\frac{9}{8}\cdot\frac{15}{16}\cdot\frac{7}{6}=\frac{315}{256}$	54	432
15	$\frac{3}{4}\cdot\frac{5}{4}\cdot\frac{35}{36}=\frac{175}{192}$	40	240
21	$\frac{3}{4}\cdot\frac{15}{16}\cdot\frac{7}{6}=\frac{105}{128}$	36	144
35	$\frac{9}{8}\cdot\frac{5}{4}\cdot\frac{7}{6}=\frac{105}{64}$	72	144
105	$\frac{3}{4}\cdot\frac{5}{4}\cdot\frac{7}{6}=\frac{35}{32}$	48	48

mean of the number of solutions of the r problems thus obtained is $(\varphi(r/d_1)\varphi(r/d_2)\dots\varphi(r/d_k))/r$. It can therefore be remarked that in (4) the number P_a, compared with 1, shows us how much the total number N_a of solutions deviates from the mean. The greater P_a, the more the class a of $\mathbf{Z}_r$ appears to be 'favored' by the expressions at the left-hand side of (1), the x_i satisfying constraints (2). According to whether $P_a > 1$ or $P_a < 1$, we can deduce that those expressions give as a result in $\mathbf{Z}_r$ the class a a number of times respectively higher or lower than the mean.

Let us remark, moreover, that for each prime divisor p of r the integer b_p is exactly the number of addenda at the left-hand side of (1) which are not multiples of p.

All this being stated, it is possible in view of (5), to deduce the following qualitative remarks:

Remark 1. For each prime divisor p of r, a sum having an even number of addenda which are not multiples of p tends to favor as possible results the multiples of p, while a sum having an odd number of addenda which

are not multiples of p tends to favor results not multiples of p.

Remark 2. If r is odd and if $h_1, h_2, \dots, h_k$, $d_1, d_2, \dots, d_k$ are fixed in such a way that, for each prime divisor p of r there are many addenda at the left-hand side of (1) which are not multiples of p, then for each class a in $\mathbf{Z}_r$, the number P_a is very close to 1. This means that in this case the distribution in $\mathbf{Z}_r$ of the values taken by the sum at the left-hand side of (1), the x_i satisfying (2), is very close to the uniform distribution. For example, the distribution in $\mathbf{Z}_r$ of the values taken by the expressions of the form $x_1 + x_2 + \cdots + x_k$ as $x_1, x_2, \dots, x_k$ vary in $\mathbf{Z}_r^*$ tends to be uniform as k tends to infinity.

4. Numerical properties of P_a. Two important values: l_v and L_v. Assuming once more that for each prime divisor p or r, $b_p \geq 1$, i.e., that for each p at least one addendum in the left-hand side of (1) exists which is not a multiple of p, the following propositions immediately derive from (5).

Proposition 1. *Once r and a are fixed, the number P_a depends only on the values taken, for each prime divisor p of r, by the number b_p, i.e., it depends exclusively on the number, for each p, of the addenda at the left-hand side of* (1) *which are not divisible by p.*

Proposition 2. *Let $k \in \mathbf{N}$ be given; let us fix a finite set of distinct prime numbers $p_1, p_2, \dots, p_t$ and define $r_0 = p_1 p_2 \dots p_t$; let us also fix $k+1$ integers $h_1, h_2, \dots, h_k$, a and k divisors $d_1, d_2, \dots, d_k$ of r_0 in such a way that for each integer j with $1 \leq j \leq t$, at least one integer w exists with $1 \leq w \leq k$ for which we have $p_j \nmid h_w d_w$. Then the number P_a is the same for every positive integer r whose prime factors are exactly $p_1, p_2, \dots, p_t$.*

After fixing a generic positive integer v, let us call I_v the set consisting of all the problems defined by equation (1) and constraints (2) with r odd and such that, for every prime divisor p of r, $b_p \geq v$. Denote by l_v and L_v the lower and upper limit, respectively (the latter being not necessarily finite) of the set of all the values which P_a may take in problems in I_v. Let us call s the greatest even integer which is not

larger than v, and t the greatest odd integer which is not larger than v. Then the following theorem holds.

Theorem 1. *For each positive integer v, in $\mathbf{R}\cup\{+\infty\}$ the equalities*

$$l_v = \prod_{\substack{p\neq 2\\ p \text{ prime}}} \left[1 - \frac{1}{(p-1)^s}\right]; \tag{6}$$

$$L_v = \prod_{\substack{p\neq 2\\ p \text{ prime}}} \left[1 + \frac{1}{(p-1)^t}\right]$$

are satisfied.

Proof. Let us consider a generic problem in I_v expressed through an equation like (1) and constraints such as (2). For every prime divisor p of r it is easy to deduce, since $b_p \geq s$ and s is even, that both the numbers $1-((-1)^{b_p}/(p-1)^{b_p})$ and $1-((-1)^{b_p-1}/(p-1)^{b_p-1})$ are not lower than $1-(1/(p-1)^s)$. Since $s \geq 0$, recalling the expression of P_a given by (5), we deduce from these latter inequalities that

$$P_a \geq \prod_{p|r}\left[1 - \frac{1}{(p-1)^s}\right] \geq \prod_{\substack{p\neq 2\\ p \text{ prime}}}\left[1 - \frac{1}{(p-1)^s}\right].$$

As this is true for every problem in I_v, we shall also have the inequality:

$$l_v \geq \prod_{\substack{p\neq 2\\ p \text{ prime}}}\left[1 - \frac{1}{(p-1)^s}\right]. \tag{7}$$

Now for a fixed generic integer $n \geq 3$, let $r = \prod_{3\leq p\leq n, p \text{ prime}} p$. We here distinguish the case in which v is even from the case in which v is odd.

First case: *v even.* In this case we have $s = v$. Let us consider the problem given by equation $x_1 + x_2 + \cdots + x_v \equiv 1 \pmod r$ and by equalities $(x_1, r) = (x_2, r) = \cdots = (x_v, r) = 1$. It is clear that for every

prime divisor p of r we have $b_p = v$: the problem is therefore contained in I_v. From equality (5) we deduce that $P_1 = \prod_{p|r}[1-(-1)^v/(p-1)^v]$, i.e.,

$$P_1 = \prod_{\substack{3\le p\le n\\ p \text{ prime}}} \left[1 - \frac{1}{(p-1)^s}\right]. \tag{8}$$

Second case: v *odd.* In this case we have $s = v - 1$. Let us consider the problem given by equation $x_1 + x_2 + \cdots + x_v \equiv 0 \pmod r$ and by equalities $(x_1, r) = (x_2, r) = \cdots = (x_v, r) = 1$. Here too for every prime divisor p of r we have $b_p = v$ and the problem is once more in I_v. We have $P_0 = \prod_{p|r}[1 - (-1)^{v-1}/(p-1)^{v-1}]$, i.e.,

$$P_0 = \prod_{\substack{3\le p\le n\\ p \text{ prime}}} \left[1 - \frac{1}{(p-1)^s}\right]. \tag{9}$$

From equalities (8), for v even, and (9), for v odd, we deduce that, whatever the value of v, a problem in I_v exists for which we have $P_a = \prod_{\substack{3\le p\le n\\ p \text{ prime}}}[1 - (1/(p-1)^s)]$. This necessarily implies that

$$l_v \le \prod_{\substack{3\le p\le n\\ p \text{ prime}}} \left[1 - \frac{1}{(p-1)^s}\right].$$

As the latter inequality holds for every integer $n \ge 3$, we can deduce, passing to the limit for n tending to infinity, that

$$l_v \le \prod_{\substack{p\ne 2\\ p \text{ prime}}} \left[1 - \frac{1}{(p-1)^s}\right]. \tag{10}$$

The first of (6) follows from (7) and (10).

By adopting a similar procedure one also proves the second equality in (6).

5. Approximations of l_v and L_v. For each positive integer i, let us denote by q_i the ith prime number (we shall have therefore $q_1 = 2$,

$q_2 = 3$, $q_3 = 5$, $q_4 = 7$, $q_5 = 11, \dots$). Now let us fix $v \geq 2$ and consider the corresponding numbers s and t. Since for each $i \in \mathbf{N}$ we clearly have $q_i \leq q_{i+1} - 1 < q_{i+1}$, the following inequalities are satisfied:

$$1 - \frac{1}{q_i^s} \leq 1 - \frac{1}{(q_{i+1}-1)^s} < 1 - \frac{1}{q_{i+1}^s} \quad \forall\, i \in \mathbf{N}, \tag{11}$$

and

$$1 + \frac{1}{q_{i+1}^t} < 1 + \frac{1}{(q_{i+1}-1)^t} \leq 1 + \frac{1}{q_i^t} \quad \forall\, i \in \mathbf{N}. \tag{12}$$

For each fixed positive integer m, resorting to (11), we can write

$$\prod_{i \geq m} \left[1 - \frac{1}{q_i^s}\right] < \prod_{i \geq m} \left[1 - \frac{1}{(q_{i+1}-1)^s}\right] < \prod_{i \geq m} \left[1 - \frac{1}{q_{i+1}^s}\right],$$

i.e.,

$$\frac{\prod_{i \in \mathbf{N}}(1 - (1/q_i^s))}{\prod_{i<m}(1 - (1/q_i^s))} < \prod_{i \geq m} \left[1 - \frac{1}{(q_{i+1}-1)^s}\right] < \frac{\prod_{i \in \mathbf{N}}(1 - (1/q_i^s))}{\prod_{i<m+1}(1 - (1/q_i^s))},$$

i.e.,

$$\frac{[\zeta(s)]^{-1}}{\prod_{i<m}(1 - (1/q_i^s))} < \prod_{i \geq m} \left[1 - \frac{1}{(q_{i+1}-1)^s}\right] < \frac{[\zeta(s)]^{-1}}{\prod_{i<m+1}(1 - (1/q_i^s))}, \tag{13}$$

$\zeta(s)$ denoting Riemann's function.

We pose $l_{v,m} = \prod_{i=1}^{m-1}[1 - (1/(q_{i+1}-1)^s)] = \prod_{3 \leq p \leq q_m, p \text{ prime}}[1 - (1/(p-1)^s)]$. From the first of equalities (6) we have $l_v = \prod_{i \in \mathbf{N}}[1 - (1/(q_{i+1}-1)^s)] = l_{v,m} \cdot \prod_{i \geq m}[1 - (1/(q_{i+1}-1)^s)]$. From inequalities (13), by multiplying all members by $l_{v,m}$, we can therefore deduce that

$$\frac{1}{\zeta(s)} \cdot \frac{l_{v,m}}{\prod_{i<m}(1 - (1/q_i^s))} < l_v < \frac{1}{\zeta(s)} \cdot \frac{l_{v,m}}{\prod_{i<m+1}(1 - (1/q_i^s))}. \tag{14}$$

If we calculate the finite product which gives the value of $l_{v,m}$ and we know the value of $\zeta(s)$, then inequalities (14) give us a good

approximation of l_v; indeed, the first member differs from l_v by a multiplicative factor lying in the interval $[1; 1/(1-q_m^{-s})]$, i.e., lying in the interval $[1; q_m^s/(q_m^s-1)]$.

By adopting a similar procedure and using the equality $1+(1/n^t) = (1-n^{-2t})/(1-n^{-t})$ for generic $n \in \mathbf{N}$, if $v \geq 3$, we can derive from (12) for each fixed $m \in \mathbf{N}$, the relations:

$$\frac{\zeta(t)}{\zeta(2t)} \cdot \frac{L_{v,m}}{\prod_{i<m+1}(1+(1/q_i^t))} < L_v < \frac{\zeta(t)}{\zeta(2t)} \cdot \frac{L_{v,m}}{\prod_{i<m}(1+(1/q_i^t))}, \tag{15}$$

where $L_{v,m} = \prod_{i=1}^{m-1}[1+(1/(q_{i+1}-1)^t)] = \prod_{3\leq p\leq q_m, p \text{ prime}}[1+(1/(p-1)^t)]$. If we calculate $L_{v,m}$ and we know the values of $\zeta(t)$ and $\zeta(2t)$, we have from (15) a good approximation of L_v in which the third member differs from L_v by a multiplicative factor lying in the interval $[1/(1+q_m^{-t}); 1]$, i.e., in the interval $[q_m^t/(q_m^t+1); 1]$.

As an example of what was treated above, by taking $v = 2$ and $m = 11$, we can deduce from (14) that $0.659 < l_2 < 0.661$.

If we do not know the values of $\zeta(s), \zeta(t)$ or $\zeta(2t)$, we can use the following theorem:

Theorem 2. *For each fixed $m \in \mathbf{N}$, we have*

$$l_{v,m} \cdot \frac{(s-1)(q_m-1)^{s-1}}{(s-1)(q_m-1)^{s-1}+1} < l_v < l_{v,m} \tag{16}$$

and, if $v \geq 3$,

$$L_{v,m} < L_v < L_{v,m} \cdot \frac{(t-1)(q_m-1)^{t-1}+1}{(t-1)(q_m-1)^{t-1}}. \tag{17}$$

Proof. For m fixed, in order to prove inequalities (16) it is sufficient to show that $\prod_{i\geq m}[1-(1/(q_{i+1}-1)^s)] > [(s-1)(q_m-1)^{s-1}]/$

$[(s-1)(q_m-1)^{s-1}+1]$. Indeed, we have

$$\begin{aligned}\prod_{i\geq m}\left[1-\frac{1}{(q_{i+1}-1)^s}\right] &> \prod_{i\geq m}\left[1-\frac{1}{q_i^s}\right] = \frac{1}{\sum_{n,[p|n\Rightarrow p\geq q_m]}(1/n^s)}\\ &\geq \frac{1}{1+\sum_{n\geq q_m}(1/n^s)} > \frac{1}{1+\int_{q_m-1}^{+\infty}x^{-s}\,dx}\\ &= \frac{1}{1+(1/(s-1)(q_m-1)^{s-1})}\\ &= \frac{(s-1)(q_m-1)^{s-1}}{(s-1)(q_m-1)^{s-1}+1}.\end{aligned}$$

To prove inequalities (17) we observe that, for fixed m,

$$\begin{aligned}\prod_{i\geq m}\left[1+\frac{1}{(q_{i+1}-1)^t}\right] &< \prod_{i\geq m}\left[1+\frac{1}{q_i^t}\right] < 1+\sum_{n\geq q_m}\frac{1}{n^t}\\ &< 1+\int_{q_m-1}^{+\infty}x^{-t}\,dx = \frac{(t-1)(q_m-1)^{t-1}+1}{(t-1)(q_m-1)^{t-1}}.\end{aligned}$$

This concludes our proof. □

As an application of Theorem 2, by taking $v=3$ and $m=8$ we obtain from (17) that $1.150 < L_3 < 1.153$.

We conclude with two final observations about l_v and L_v. First let us fix $v\geq 3$ and consider a problem in I_v; let N_a be the number of solutions of such a problem. Let us now modify in this problem only the element a, say $a\to b$, keeping unchanged all the other variables and conditions; let N_b be the number of solutions of the new problem. We consider the ratio N_a/N_b. v being fixed, by resorting to the proof of Theorem 1 it can be noticed that, whatever the value of v, two successions are built, say $(\gamma_n)_{n\in\mathbf{N}}$ and $(\delta_n)_{n\in\mathbf{N}}$, of problems in I_v, where for each $n\in\mathbf{N}$ the only difference between γ_n and δ_n is the class at the righthand side of (1). The limit of the value P_a associated to γ_n when $n\to+\infty$ is l_v, while the limit of P_a associated to δ_n when $n\to+\infty$ is L_v. All this implies that the upper limit of all the possible values N_a/N_b which we can obtain in the way described above is the ratio L_v/l_v.

The second observation concerning l_v and L_v is qualitative. Being l_v and L_v the lower and upper limit, respectively, of the values which P_a

may take in problems in I_v, recalling what was observed about P_a at the beginning of Section 3, we can say that l_v and L_v, compared with 1, represent the limits (which can never be exactly reached if $v \geq 2$) of the possible deviations from the mean of the frequencies of the values taken by a sum in which there are, for each prime number $p \geq 3$ lying in a finite set E, at least v addenda not multiples of p.

REFERENCES

1. U. Cerruti, *Counting the number of solutions of congruences*, in *Application of Fibonacci numbers* (G.E. Bergum, et al., eds.), Kluwer Acad. Publ., Dordrecht, 1993.

2. P.J. McCarthy, *Introduction to arithmetical functions*, Springer-Verlag, New York, 1986.

3. R. Sivaramakrishnan, *Classical theory of arithmetic functions*, Marcel Dekker, New York, 1989.

4. D. Ugrin-Šparac, *On a class of enumeration problems in additive arithmetics*, J. Number Theory **45** (1993), 117–128.

Istituto Di Informatica E Telematica, Area Della Ricerca CNR, Via Giuseppe Moruzzi 1, 56124 Pisa, Italy
E-mail address: giovanni.sburlati@iit.cnr.it