THE NUMBER OF SOLUTIONS TO $ax + by = n$

Amitabha Tripathi
Dept. of Mathematics, Indian Institute of Technology, New Delhi 110016, India
atripath@maths.iitd.ernet.in
(Submitted August 1998-Final Revision May 1999)

In this note we determine an exact formula for the number of solutions, $N(a,b;n)$ in nonnegative integer pairs (x,y) of the equation $ax+by=n$ if $\gcd(a,b)=1$. There is no loss of generality in this since $ax+by=n$ is solvable if and only if $d \doteq \gcd(a,b) \mid n$, so that the number of solutions in general would be given by $N(\frac{a}{d}, \frac{b}{d}; \frac{n}{d})$. It is well known that $N(a,b;n)$ is always one of the two consecutive integers $\lfloor \frac{n}{ab} \rfloor$ or $\lfloor \frac{n}{ab} \rfloor + 1$; see, for instance [3, page 214] or [4, page 90]. A history of this and related problems may be found in [2, pages 64-71]. In this note we shall henceforth assume that a, b are positive, relatively prime integers, that n is a nonnegative integer, and prove the following

Theorem:

$$N(a,b;n) = \frac{n + aa'(n) + bb'(n)}{ab} - 1,$$

where $a'(n) \equiv -na^{-1} \pmod{b}$, $1 \le a'(n) \le b$, $b'(n) \equiv -nb^{-1} \pmod{a}$, $1 \le b'(n) \le a$.

We observe that $n + bb'(n)$ is a multiple of a and that $n + aa'(n)$ is a multiple of b. Therefore, $n + aa'(n) + bb'(n)$ is a multiple of ab, and is at least $n+a+b$. It follows that the expression that represents $N(a,b;n)$ in the theorem is indeed a nonnegative integer.

We prove our result in two ways. Our first method uses generating functions to determine the function $N(a,b;n)$, while the second method verifies the formula just obtained by showing that this function meets the characterizing properties that such a function should satisfy.

We begin our first proof by observing that $N(a,b;n)$ equals the coefficient of x^n in the expansion of $(1-x^a)^{-1}(1-x^b)^{-1}$. Also, since $x^m - 1 = \prod_{k=1}^{m}(x - \zeta_m^k)$, we have

$$1 - x^m = \prod_{k=1}^{m}(1 - \zeta_m^{-k}x),$$

where $\zeta_m \doteq e^{2\pi i/m}$.

We write

$$\begin{aligned}\mathcal{N}(x) \doteq \sum_{n \ge 0} N(a,b;n)x^n &= \frac{1}{(1-x^a)(1-x^b)} \\ &= \frac{c_1}{1-x} + \frac{c_2}{(1-x)^2} + \sum_{k=1}^{a-1} \frac{A_k}{1-\zeta_a^{-k}x} + \sum_{k=1}^{b-1} \frac{B_k}{1-\zeta_b^{-k}x},\end{aligned} \tag{1}$$

where $\zeta_a \doteq e^{2\pi i/a}$ and $\zeta_b \doteq e^{2\pi i/b}$.

In (1) and elsewhere, we adopt the usual convention of assigning the value 0 to any empty sum and the value 1 to any empty product. Comparing coefficients of x^n, we have

$$N(a,b;n) = c_1 + c_2(n+1) + \sum_{k=1}^{a-1} A_k \zeta_a^{-nk} + \sum_{k=1}^{b-1} B_k \zeta_b^{-nk}. \tag{2}$$

A simple calculation shows that $c_1=(a+b-2)/2ab$ and $c_2=1/ab$. Evaluation of the A_k's and the B_k's is done by multiplying both sides of (1) by the corresponding $1-\zeta^{-k}x$ and taking limits as $x\to\zeta^k$. This yields $A_k=1/a(1-\zeta_a^{bk})$, with a similar expression for the B_k's.

From (2),

$$N(a,b;n)=\frac{n}{ab}+\frac{a+b}{2ab}+\frac{1}{a}\sum_{k=1}^{a-1}\frac{\zeta_a^{-nk}}{1-\zeta_a^{bk}}+\frac{1}{b}\sum_{k=1}^{b-1}\frac{\zeta_b^{-nk}}{1-\zeta_b^{ak}}. \tag{3}$$

We observe that each sum on the right is periodic in n, the first with period a and the second with period b. Since a and b are coprime, the two sums together has a period ab, and the expression for $N(a,b;n)$ is essentially determined modulo ab. The form that the function $N(a,b;n)$ takes is well known; see [4, page 90] and [1, pages 113-14].

Notation: We set $a'(n)\equiv -na^{-1}\pmod b$, $b'(n)\equiv -nb^{-1}\pmod a$, with $1\le a'(n)\le b$, $1\le b'(n)\le a$.

We note that $\sum_{k=1}^{a-1}\zeta_a^{mk}=\sum_{k=0}^{a-1}\zeta_a^{mk}-1=-1$ for any integer m that is not a multiple of a; it equals $a-1$ otherwise.

From $\sum_{k=0}^{a-1}x^k=\prod_{k=1}^{a-1}(x-\zeta_a^k)$, logarithmic differentiation at $x=1$ gives $\sum_{k=1}^{a-1}(1-\zeta_a^k)^{-1}=(a-1)/2$ if $a\ge 2$. The equation is also trivially valid for $a=1$.

Since $(1-\zeta_a^{bk})(1+\zeta_a^{bk}+\zeta_a^{2bk}+\cdots+\zeta_a^{(b'-1)bk})=1-\zeta_a^{b'bk}=1-\zeta_a^{-nk}$, we have

$$\begin{aligned}\sum_{k=1}^{a-1}\frac{\zeta_a^{-nk}}{1-\zeta_a^{bk}}&=-\sum_{k=1}^{a-1}(1+\zeta_a^{bk}+\zeta_a^{2bk}+\cdots+\zeta_a^{(b'-1)bk})+\sum_{k=1}^{a-1}\frac{1}{1-\zeta_a^{bk}}\\&=-[(a-1)-(b'-1)]+\sum_{k=1}^{a-1}\frac{1}{1-\zeta_a^{k}}\\&=b'-a+\frac{a-1}{2}=b'-\frac{a+1}{2},\quad\text{where } b'=b'(n).\end{aligned}$$

Putting all this into (3), we have

$$\begin{aligned}abN(a,b;n)&=\frac{a+b}{2}+n+b\left(b'(n)-\frac{a+1}{2}\right)+a\left(a'(n)-\frac{b+1}{2}\right)\\&=aa'(n)+bb'(n)-ab+n,\end{aligned}\tag{4}$$

which completes the proof of our result.

We now prove that the following four properties, stated in the Proposition below and which *uniquely* characterize the function $N(a,b;n)$, are satisfied by the expression given in the Theorem, thus providing a second proof of the Theorem. It is well known that the function which counts the number of nonnegative integer solutions of $ax+by=n$ must satisfy these properties; see, for instance, [4, pages 87-91].

Proposition: The function $N(a,b;n)$ is the unique function satisfying the four conditions:

$$\begin{array}{lcll} N(a,b;n+k\cdot ab) &=& N(a,b;n)+k & \text{if } k\ge 0;\\ N(a,b;n) &=& 1 & \text{if } ab-a-b<n<ab;\\ N(a,b;p)+N(a,b;q) &=& 1 & \text{if } p+q=ab-a-b,\ p,q\ge 0;\\ N(a,b;n) &=& 1 & \text{iff } n=ax_0+by_0<ab-a-b,\ x_0,y_0\ge 0.\end{array}$$

For convenience, we now use the notation

$$N'(a,b;n)=\frac{n+aa'(n)+bb'(n)}{ab}-1.$$

Lemma 1: $N'(a,b;n+k\cdot ab)=N'(a,b;n)+k$ for all integers $k\geq 0$.

Proof: Although this is an immediate consequence of (2), we also give a proof that involves the expression for $N(a,b;n)$ given by the Theorem.

$$\begin{aligned}ab\cdot N'(a,b;n+k\cdot ab)&=(n+k\cdot ab)+aa'(n+k\cdot ab)+bb'(n+k\cdot ab)-ab\\&=(n+aa'(n)+bb'(n)-ab)+k\cdot ab\\&=ab\cdot N'(a,b;n)+k\cdot ab.\ \square\end{aligned}$$

Lemma 2: $N'(a,b;n)=1$ if $ab-a-b<n<ab$.

Proof: If $ab-a-b<n<ab$, then $ab<n+a+b\leq n+aa'(n)+bb'(n)\leq n+ab+ab<3ab$, so that $n+aa'(n)+bb'(n)=2ab$ and $N'(a,b;n)=1$. $\square$

Lemma 3: If p and q are nonnegative integers such that $p+q=ab-a-b$, then $N'(a,b;p)+N'(a,b;q)=1$.

Proof: We note that $a'(p)+a'(q)\equiv 1 \pmod{b}$, so that $a'(p)+a'(q)=b+1$ since each is at least 1; similarly, $b'(p)+b'(q)=a+1$. Therefore,

$$\begin{aligned}ab\cdot N'(a,b;p)+ab\cdot N'(a,b;q)&=(aa'(p)+aa'(q))+(bb'(p)+bb'(q))-2ab+(p+q)\\&=a(b+1)+b(a+1)-(ab+a+b)\\&=ab.\ \square\end{aligned}$$

We observe that Lemma 3 asserts that exactly one of n and $ab-a-b-n$ is of the form ax_0+by_0 with $x_0,y_0\geq 0$, if $0\leq n\leq ab-a-b$. Therefore, any n which is not representable by a and b is of the form $ab-a-b-(ax_1+by_1)$, with $0\leq x_1\leq b-1$, $0\leq y_1\leq a-1$.

Lemma 4: For n such that $0\leq n\leq ab-a-b-1$,

$$N'(a,b;n)=\begin{cases}1 & \text{if } n=ax_0+by_0 \text{ for some } x_0,y_0\geq 0;\\ 0 & \text{otherwise.}\end{cases}$$

Proof: If there exist nonnegative integers x_0,y_0 such that $ax_0+by_0=n$, then $x_0\leq b-1$ and $y_0\leq a-1$, and we have

$$\begin{aligned}ab\cdot N'(a,b;n)&=(ax_0+by_0)+aa'(ax_0+by_0)+bb'(ax_0+by_0)-ab\\&=(ax_0+by_0)+a(b-x_0)+b(a-y_0)-ab\\&=ab.\end{aligned}$$

Otherwise, $n=ab-a-b-(ax_1+by_1)$ with $0\leq x_1\leq b-1$, $0\leq y_1\leq a-1$, and we have

$$\begin{aligned}ab\cdot N'(a,b;n)&=aa'(ab-a-b-ax_1-by_1)+bb'(ab-a-b-ax_1-by_1)\\&\quad-ab+(ab-a-b-ax_1-by_1)\\&=aa'(-a-ax_1)+bb'(-b-by_1)-(a+b+ax_1+by_1)\\&=a(1+x_1)+b(1+y_1)-(a+b+ax_1+by_1)=0.\ \square\end{aligned}$$

Lemmas 1-4 together show that the formula given by our Theorem meets the conditions that $N(a,b;n)$ satisfies, thereby completing our second (and less direct) proof.

An interesting consequence of our result is a solution of a special case of the *Coin Exchange Problem*. If we restrict x, y to be nonnegative, it is well known that the equation $ax+by=n$ always has a solution for all sufficiently large n. This means that the set

$$\mathcal{S}(a,b) \doteq \mathbb{N}\setminus\{ax+by : x, y \geq 0\}$$

is *finite*. The two functions

$$g(a,b) \doteq \max_{n\in\mathcal{S}} n \quad \text{and} \quad n(a,b) \doteq |\mathcal{S}|$$

can be evaluated readily from the function $N(a,b;n)$, as we now show in the following

Corollary:

(a) $g(a,b) = ab-a-b$;

(b) $n(a,b) = (a-1)(b-1)/2$.

Proof: By Lemma 4, or directly, $N(a,b;0)=1$, so that $N(a,b;ab-a-b)=0$ by Lemma 3, while $N(a,b;n)\geq 1$ if $n>ab-a-b$ by Lemmas 1 and 2. This establishes (a).

Lemma 3 implies that there is a one-to-one correspondence between representable and non-representable integers between 0 and $ab-a-b$, and (b) follows from (a). □

ACKNOWLEDGMENT

The author is grateful for initial discussions with Professor Steve Schanuel which resulted in a formula that was more intriguing than this. He is also grateful to Professor M. Ram Murty for some helpful discussion and to the referee for suggestions on improvement of the original manuscript.

REFERENCES

1. Louis Comtet. *Advanced Combinatorics*. Dordrecht: D. Reidel, 1974.
2. L. E. Dickson. *History of the Theory of Numbers*. Vol. II. New York: Chelsea, 1992.
3. Ivan Niven, Herbert S. Zuckerman, & Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. 5th ed. New York: John Wiley & Sons, 1991.
4. Herbert S. Wilf. *Generatingfunctionology*. New York: Academic Press, 1990.

AMS Classification Numbers: 11D04, 05A15

❖❖❖