and inversive geometers have delighted, but which they have signally failed to popularize, are now to be almost a commonplace in the wider field of differential geometry. The physicists who would not look at the projective gnats will swallow the differential camels. And there is no doubt more nutriment in a camel. There will be a lively market, and it should be met by some recasting where pedagogic reasons already exist. The mapping of spaces should be led up to by the simplest cases of mapping. Once again, what pedagogy sighed for physical science demands, this time in the field of elementary geometry itself.

If the science should be taught in its early stages not as a jumble of special applications, but always with an honest consideration of its legitimate contexts, then would it still be true of the far wider mathematics of today, that, to quote old Isaac Barrow again, "The Mathematics is the unshaken Foundation of Science and the Plentiful Fountain of Advantage in Human Affairs."

JOHNS HOPKINS UNIVERSITY.

FALLACIES AND MISCONCEPTIONS IN DIOPHANTINE ANALYSIS.

BY PROFESSOR L. E. DICKSON.

(Read before the American Mathematical Society March 26, 1921.)

§ 1. *Introduction.* Numerous writers have claimed to find all integral solutions of various homogeneous equations when they have actually found merely the rational solutions, expressed by formulas involving rational parameters. They have really left untouched the more difficult problem of finding all the integral solutions exclusively. The fallacies exposed in § 2 and § 3 are merely particular instances of the wide-spread misconception of the problem of solving a homogeneous equation in integers. It is therefore not safe, without reexamination, to place confidence in any claim that a homogeneous equation has been completely solved in integers.

In the next number of this BULLETIN, I shall show how the

theory of ideals can be applied to find all the solutions in integers of the homogeneous equation $x^2 + ay^2 + bz^2 = w^2$.

§ 2. *A Fallacy concerning Pairs of Equations.* It has been regarded as self-evident by all writers,* who have mentioned the topic, that the problem of solving a non-homogeneous equation in rational numbers is equivalent to the problem of solving the corresponding homogeneous equation in integers. Let us examine this question for the particular homogeneous equation

$$x^2 + 5y^2 = zw \tag{1}$$

and the corresponding non-homogeneous equation

$$X^2 + 5Y^2 = Z. \tag{2}$$

The problem of solving the latter in rational numbers is trivial. But the problem of solving (1) in integers involves the finding of all divisors of all numbers that can be represented by $x^2 + 5y^2$, which is one of the serious questions in the theory of quadratic forms. This problem will be treated in the next number of the BULLETIN by the theory of ideals; the conclusion is quoted at the end of § 4 below.

It is clear that there must be some fallacy in the customary argument that two such problems are equivalent.† This argument is the following simple one. If x, y, z, w $(w \neq 0)$ are integers satisfying (1) and if we write

$$\frac{x}{w} = X, \qquad \frac{y}{w} = Y, \qquad \frac{z}{w} = Z, \tag{3}$$

we obtain rational numbers satisfying (2). Conversely, if X, Y, Z are rational numbers satisfying (2), we may express them as fractions (3) with a common denominator and obtain integers x, y, z, w satisfying (1).

Here there is nothing wrong with the algebraic work, nor with the facts deduced. The fallacy lies in the failure to perceive that these facts do not warrant the conclusion that, in the converse case, we have shown how to find all integral solutions. That goal requires that we find all integers w such that the products wX, wY, wZ are integers, viz., x, y, and z. All such integers w are evidently multiples of the minimum

* Including Gauss, *Disquisitiones Arithmeticae*, § 300.

† Namely, that any solution of one equation corresponds to solutions of the other equation under the transformation (3).

positive integer w. To find the minimum w, we need the least common denominator l of the fractions X, Y, and Z. Let d denote the least common denominator of the fractions X and Y, so that $X = \xi/d$, $Y = \eta/d$, where ξ, η, and d are integers without a common factor > 1. Then we have

$$Z = \frac{\xi^2 + 5\eta^2}{d^2}.$$

Before we can find l, we must find the irreducible fraction which equals Z. But this requires the knowledge of all the divisors of all numbers that can be represented by $\xi^2 + 5\eta^2$. Hence we have made no real advance over our initial problem (1) by utilizing our knowledge of the complete solution in rational numbers of the corresponding non-homogeneous equation (2).

§ 3. *The Fallacy when both Equations are Homogeneous.* There is a wide-spread belief that the problem of finding all rational solutions of a homogeneous equation is equivalent to that of finding all its integral solutions. The argument was recently restated by a specialist as follows: (i) the set of all rational solutions contains the set of all integral solutions, and (ii) from the set of all integral solutions it is obvious that the set of all rational solutions is obtained by dividing the numbers in each solution by an arbitrary positive integer.

But remark (i) does not serve the purpose intended, since it leaves unanswered the vital question of how to select the infinitude of integral solutions from the rational solutions. The futility of the argument is emphasized by replacing (i) by the equally trivial remark that all integral solutions occur among the real (or complex) solutions.

In order to bring out clearly the distinction between the two problems, consider the special equation (1). Its rational solutions are obviously all included in the following two types: $x = y = z = 0$, with w any rational number; and x, y, z any rational numbers such that $z \neq 0$, with $w = (x^2 + 5y^2)/z$. We have therefore solved by inspection our first problem of finding all the rational solutions.

Does this information alone serve, as claimed, to yield the complete solution of our second problem of finding all the integral solutions of equation (1)? If so, we should be able, without further theory, to pick out the integral solutions from

the preceding rational solutions. This is easily done for the first type of rational solutions; we have only to restrict w to integral values. For the second type, we must not only restrict x, y, and z to integral values, but we must also examine the condition that $x^2 + 5y^2$ shall be divisible by z. Expressed otherwise, we require a process, valid for arbitrary integers x and y, of finding all divisors z of $x^2 + 5y^2$ (the quotients giving the corresponding values of w). Since we have merely returned to a restatement of our second problem of finding all the integral solutions of (1), we have made no advance whatever on that problem by considering the first problem of finding the rational solutions.

§ 4. *A common Misconception concerning Integral Solutions of a Homogeneous Equation.* To have a concrete case in point, let us express the rational solutions of equation (1) in the customary homogeneous form, which has the advantage of combining into a single formula the two preceding types of solutions. For $z \neq 0$, express x, y, and z as fractions with the positive least common denominator l, and let n be the greatest common divisor of the numerators. Then

$$(4) \quad x = \frac{na}{l}, \qquad y = \frac{nb}{l}, \qquad z = \frac{nc}{l}, \qquad w = \frac{n(a^2 + 5b^2)}{cl},$$

where a, b, and c are integers without a common factor > 1, while n and l are integers without a common factor > 1, and $cl \neq 0$. Write ρ for $n/(cl)$. Then

$$(5) \qquad x = \rho ac, \quad y = \rho bc, \quad z = \rho c^2, \quad w = \rho(a^2 + 5b^2).$$

The solutions with $z = 0$ have $x = y = 0$ and are of the form (5) with $c = 0$. Hence all rational solutions of (1) are given by (5), in which a, b, and c are integers without a common factor, while ρ is rational.

Some writers are in the habit of suppressing the *proportionality factor* ρ and claiming without further examination that the resulting values give the general solution in integers. Essentially the same error vitiates the claim of Desboves* that he obtains the complete solution in integers of the general homogeneous quadratic equation in n unknowns when one solution $x, y, \cdots$ is given. Since he regarded $mx, my, \cdots$ as the same solution as $x, y, \cdots$, where m is rational, it is clear

* NOUVELLES ANNALES, (3), vol. 3 (1884), pp. 225–39.

that he found at most formulas for the rational* solutions. Thus he deliberately prevented himself from even attacking the far more difficult problem of finding the integral solutions, though he claimed to find them.

For most homogeneous equations the true state of affairs is analogous to what we shall show to be the case for our special equation (1). Unfortunately we do not obtain all integral solutions if we restrict ρ to integral values in (5), but we must employ values whose denominators increase without limit.

By a certain simplification we shall place in its most favorable light the question of describing all sets of numbers a, b, c, and ρ (with a, b, and c integers without a common factor, and ρ rational) for which the solution (5) is integral, and we shall show that there remains an essential difficulty in the determination of these sets. First, if $c = 0$, then $x = y = z = 0$, and w may be identified with any assigned integer k by taking $\rho = k$, $a = 1$, $b = 0$, for example. Next, let $c \neq 0$. Returning from (5) to the equivalent form (4), we see that x, y, z, w are integers if and only if $l = +1$ and $n(a^2 + 5b^2)$ is divisible by c, whence $\rho = n/c$. Eliminating n, we see† that the conditions on a, b, c, and ρ are that ρc and $\rho(a^2 + 5b^2)$ be integers.‡ Hence the infinitude of sets of numbers a, b, c, and ρ for which formulas (5) give integers, and hence give all integral solutions of (1), may be *described* as follows: (i) the sets $a = 1$, $b = c = 0$, with ρ integral; (ii) the sets for which a, b, and c ($c \neq 0$) range over all triples of integers without a common factor, while for each triple ρ ranges over all the irreducible fractions whose denominators are common divisors of c and $a^2 + 5b^2$. But we have not shown how to *determine* the sets a, b, c, and ρ just described. Their determination requires the finding of all divisors of all numbers represented by the quadratic form $a^2 + 5b^2$. Our simplified description of the integral solutions on the basis for the formulas (5) for the

* But these can be found at once by considering all the lines through the given rational point.

† Also direct from (5) by using the theorem that, if a, b, c have the greatest common divisor 1, integers A, B, C may be found such that $aA + bB + cC = 1$. Multiply by ρc and apply (5). Thus $xA + yB + zC = \rho c$ = integer.

‡ It is now easily proved that the denominators of the ρ's are unlimited. As is known, there is an infinitude of primes p of the form $\alpha^2 + 5\beta^2$. To obtain the solution $x = \alpha$, $y = \beta$, $z = p$, $w = 1$ by (5), we must take the integral factors ρc and c of z to be ± 1 and $\pm p$, whence $\rho = 1/p$, since the choice $\rho c = \pm p$, $c = \pm 1$ would give $\rho = p$, $w > 1$.

rational solutions is therefore no essential improvement upon the description which the proposed equation itself may be said to give.

In accord with the theory to be explained in the next number of this BULLETIN, the successful determination of the integral solutions is made on the basis of a study, not of formulas (5) for the rational solutions, but of the new formulas

$$\begin{aligned} x &= \rho(ac - 5bd), & z &= \rho(c^2 + 5d^2), \\ y &= \rho(ad + bc), & w &= \rho(a^2 + 5b^2), \end{aligned} \tag{6}$$

which reduce to (5) when $d = 0$ and hence give all the rational solutions. What really happens is well explained in the language of medicine: the injection of the additional integral parameter* d into our solution (5) counteracts the irritation caused by the rational ρ's with their infinitude of denominators. To prevent confusion in a comparison with (6), rewrite (6) in new letters:

$$\begin{aligned} x &= \sigma(AC - 5BD), & z &= \sigma(C^2 + 5D^2), \\ y &= \sigma(AD + BC), & w &= \sigma(A^2 + 5B^2). \end{aligned} \tag{7}$$

We now attempt to describe all sets of numbers A, B, C, D, and σ (with A, B, C, and D integers without a common factor, and σ rational) for which formulas (7) give integers and hence give all integral solutions of (1). When σ is integral, there is no additional restriction on the integers A, B, C, and D. When σ is an irreducible fraction with the denominator 2, the numbers (7) are all integers if and only if $C \equiv D$, $A \equiv B \pmod 2$. Hence we write

$$D = q,\ C = 2l + q,\ B = r,\quad A = 2n - r,\ \sigma = \tfrac{1}{2}\rho,$$

and we obtain

$$\begin{aligned} x &= \rho(2ln - lr + nq - 3qr), & y &= \rho(lr + nq), \\ z &= \rho(2l^2 + 2lq + 3q^2), & w &= \rho(2n^2 - 2nr + 3r^2), \end{aligned} \tag{8}$$

* It is rationally redundant. Any given solution (7), which is (6) written in new letters can be expressed in the form (5). If $C = D = 0$, whence $x = y = z = 0$, take $c = 0$ and identify the two w's, which can be done in infinitely many ways. If C and D are not both zero, take

$$a = (AC - 5BD)/t, \quad b = (AD + BC)/t, \quad c = (C^2 + 5D^2)/t, \quad \rho = t\sigma/c,$$

where t is the greatest common divisor of the three numbers whose division by t is indicated. Our former conditions that ρc and $\rho(a^2 + 5b^2)$ be integers now require that σt and $\sigma(A^2 + 5B^2)$ be integers.

where l, q, n, and r are integers without a common factor, and ρ is an integer.* Next, if σ is an irreducible fraction $\rho/5$ with the denominator 5, the numbers (7) are all integers if and only if C and A are divisible by 5. Writing $A = 5b$, $C = -5d$, $B = -a$, $D = c$, we obtain (6). A more typical case is that in which σ is an irreducible fraction of the form $\rho/3$. Then the numbers (7) are all integers if and only if we have $C \equiv D$, $A \equiv \pm B \pmod 3$. Writing $C = \pm D + 3d$, $A = \mp B + 3b$ in (7), we obtain

$$(9)\qquad \begin{aligned} x &= \rho(3bd \pm bD \mp dB - 2BD), \qquad y = \rho(bD + dB), \\ z &= \rho(2D^2 \pm 2Dd + 3d^2), \qquad w = \rho(2B^2 \mp 2Bb + 3b^2). \end{aligned}$$

For the lower signs, we replace D by l, d by $-q$, B by $-n$, b by r, and obtain (8). For the upper signs, we replace D by $l+q$, d by $-q$, B by $r-n$, b by r, and again obtain (8).

In our next paper we shall show how to construct a machine which examines in this manner each of the infinitude of cases corresponding to the values of the denominators of all irreducible fractions σ, and we shall prove that the solutions which result from any denominator are identical with the solutions (6) and (8) which resulted from the denominators 1 and 2. It will then follow that (6) and (8) together give all the integral solutions of (1) when all the parameters take only integral values.

The goal just reached for our example (1) indicates the desirable form for the integral solutions of any homogeneous equation, viz. expressibility by one or more sets of formulas involving only integral parameters. As in our example, the two sets of formulas (6) and (8) which together give all the integral solutions, may be combined, by way of abbreviation, into a single set of formulas (6) in which the denominator of the only non-integral parameter ρ is limited to the values 1 and 2. Conversely, when it is claimed that all integral solutions of a homogeneous equation† are given by formulas

* Not all solutions (8) are included among solutions (6). When $l = q = n = r = \rho = 1$, (8) gives $x = -1$, $y = 2$, $z = 7$, $w = 3$. If this solution were of the form (6) for integral a, b, c, d, ρ, then $\rho = \pm 1$ by $x = -1$, and, by $z = 7$, $\pm(c^2 + 5d^2) = 7$, which is impossible in integers.

† As to its rational solutions, if we except the rare cases in which recurring series are used, when a homogeneous equation has been completely solved in rational numbers, the unknowns x_1, x_2, $\cdots$ are expressed as homogeneous polynomials f_i, with integral coefficients, of the same degree in certain independent rational parameters A, B, $\cdots$. Writing $A = ka$,

involving a rational parameter, it should be in the sense of an abbreviated statement with explicit indication of easily performable operations leading to formulas containing only integral parameters. Strictly speaking, we do not produce a solution in integers except by a finite number of additions and multiplications performed upon independent integral parameters. These statements are in accord with the evident intention of writers on this subject, even though their conclusions are not proved and very frequently are erroneous.

§ 5. *A Theorem concerning Pairs of Equations.* By way of contrast with § 2, § 3, we note that it is true that the problem of solving any Diophantine equation in rational numbers is equivalent to the problem of solving the corresponding homogeneous equation in rational numbers. In fact, by definition we can pass from the one equation to the other by a substitution like (3). Thus, if x, y, z, w $(w \neq 0)$ give a rational solution of the homogeneous equation, then X, Y, Z give a rational solution of the corresponding equation. Conversely, any rational solution X, Y, Z of the latter gives the solution $x = wX$, $y = wY$, $z = wZ$, w of the homogeneous equation, where w is any rational number. Here there is no delicate question of sorting out solutions of a desired type from those initially obtained.

THE UNIVERSITY OF CHICAGO,
February 15, 1920.

$B = kb, \cdots$, where $a, b, \cdots$ are integers without a common factor, we obtain

$$x_1 = \rho f_1(a, b, \cdots), \qquad x_2 = \rho f_2(a, b, \cdots), \quad \cdots,$$

where ρ alone takes rational values. If a homogeneous equation in three unknowns represents a unicursal curve (of genus zero), its rational solutions must be of this form, as shown by Hilbert and Hurwitz, ACTA MATHEMATICA, vol. 14 (1890–1), pp. 217–24. Some writers have expressed their solutions as non-homogeneous polynomials in parameters $p_1, \cdots, p_k$; to pass to homogeneous polynomials, we have only to use new parameters $P, P_1 = p_1/P, \cdots, P_k = p_k/P$. One writer used parameters subject to an equation of condition, which a later writer solved, and passed to independent parameters. The case of dependent parameters is a preliminary stage in the treatment of the problem. For details on these points, with references, see the writer's *History of the Theory of Numbers*, vol. 2 (*Diophantine Analysis*), Carnegie Institution of Washington, 1920, pp. 556–8, 646, 675–6, 695.