ON BELL'S ARITHMETIC OF BOOLEAN ALGEBRA[*]

BY

WALLIE ABRAHAM HURWITZ

1. **Introduction.** Bell[†] has constructed an arithmetic for an algebra of logic or (following the terminology of Sheffer[‡]) a Boolean algebra, which presents gratifying analogies to the arithmetics of rational and other fields. In only one detail is the similarity less close than seems appropriate to the difference in the structures of the algebras themselves—namely, in the properties of the concept *congruence*. In this note I shall show that a slightly more general definition retains all the properties of the congruence given by Bell and restores several analogies to rational arithmetic lost by the Bell definition.

All the notation and terminology of the paper of Bell (to which reference should be made for results not here repeated) other than those relating to congruence are followed in the present treatment. In particular, we utilize the two (dual) interpretations of arithmetic operations and relations in $\mathfrak{L}$:

	Name	Symbol	Interpretation I	Interpretation II
(s)	Arithmetic sum:	$\alpha s\beta$:	$\alpha+\beta$,	$\alpha\beta$;
(p)	Arithmetic product:	$\alpha p\beta$:	$\alpha\beta$,	$\alpha+\beta$;
(g)	G. C. D.:	$\alpha g\beta$:	$\alpha+\beta$,	$\alpha\beta$;
(l)	L. C. M.:	$\alpha l\beta$:	$\alpha\beta$,	$\alpha+\beta$;
(ζ)	Arithmetic zero:	ζ:	ω,	ϵ;
(v)	Arithmetic unity:	v:	ϵ,	ω;
(d)	α divides β:	$\alpha d\beta$:	$\alpha \mid \beta$,	$\beta \mid \alpha$.

2. **Residuals.** It will be convenient to amplify slightly Bell's treatment of residuals. By the residual of b with respect to a in $\mathfrak{A}$, bra, is meant the quotient of a by the G. C. D. of a and b. Transforming this into a form equivalent for $\mathfrak{A}$ and suitable, by the non-appearance of the concept quotient, for analogy in $\mathfrak{L}$, Bell uses for $\mathfrak{L}$ substantially the following: $\beta r\alpha$ is the G. C. D. of all λ such that α divides the arithmetic product of λ and β. If we use interpretation I, we have that $\beta r\alpha$ is the algebraic (in this case also arithmetic) sum of all λ such that $\alpha \mid \lambda\beta$. But for any such λ, $\lambda\beta\alpha = \lambda\beta$,

[*] Presented to the Society, April 7, 1928; received by the editors August 20, 1927.

[†] E. T. Bell, *Arithmetic of logic*, these Transactions, vol. 29 (1927), pp. 597–611.

[‡] H. M. Sheffer, *A set of five independent postulates for Boolean algebras with applications to logical constants*, these Transactions, vol. 14 (1913), pp. 481–488.

for which it is necessary and sufficient that $\lambda=\xi(\alpha+\beta')$, where ξ is any element of $\mathfrak{L}$. The sum of all such λ is $\alpha+\beta'$.

If we adopt interpretation II, we find similarly that the residual of β with respect to α is $\alpha\beta'$. We may thus add to the table of interpretations

(r) Residual: $\beta r\alpha$: $\alpha+\beta'$, $\alpha\beta'$.

For both interpretations we may write

$$\beta r\alpha = \alpha s\beta'.$$

3. **Congruence.** In rational number theory the assertion $a\equiv b \bmod m$ means that $a-b$ is divisible by m. If we desire to remain within the set of non-negative rational integers, we may say that $a\equiv b \bmod m$ if there exist c, x, y such that $a=c+mx$, $b=c+my$. We adopt correspondingly as the definition for $\mathfrak{L}$, in place of Bell's (1.1)-(1.7):

$$\alpha\equiv\beta \bmod \mu \text{ if there exist } \gamma,\ \xi,\ \eta \text{ such that } \alpha=\gamma s(\mu p\xi),\ \beta=\gamma s(\mu p\eta).$$

We shall see that this definition satisfies Bell's (1.1)-(1.4) and the Boolean analogies of his (1.5), (1.6) just as do his own interpretations (4.1), (4.2), gives even a better analogy for his (1.7), and preserves several other important analogies with rational arithmetic which otherwise fail.

Under interpretation I we have for $\alpha\equiv\beta \bmod \mu$

$$\alpha = \gamma + \mu\xi, \quad \beta = \gamma + \mu\eta.$$

Multiplying (algebraically) by μ', we find $\alpha\mu'=\gamma\mu'$, $\beta\mu'=\gamma\mu'$; hence $\alpha\mu'=\beta\mu'$. But conversely this condition is sufficient for $\alpha\equiv\beta \bmod \mu$; for if $\alpha\mu'=\beta\mu'$, we may choose $\gamma=\alpha\mu'=\beta\mu'$, $\xi=\alpha$, $\eta=\beta$.

Under interpretation II we find similarly that for $\alpha\equiv\beta \bmod \mu$ it is necessary and sufficient that $\alpha+\mu'=\beta+\mu'$. We therefore replace Bell's interpretations by the following:

(c) $\alpha \equiv \beta \bmod \mu$: $\alpha\mu' = \beta\mu'$, $\alpha + \mu' = \beta + \mu'$.

In both cases, $\alpha\equiv\beta \bmod \mu$ *if and only if* $\alpha p\mu'=\beta p\mu'$.

4. **Satisfaction of Bell's conditions.** The first four of Bell's conditions (1.1)-(1.4), stated directly for $\mathfrak{L}$ in terms of the congruence notation, are as follows:

If $\alpha\equiv\beta \bmod \mu$, then $\beta\equiv\alpha \bmod \mu$.
If $\alpha\equiv\beta \bmod \mu$ and $\beta\equiv\gamma \bmod \mu$, then $\alpha\equiv\gamma \bmod \mu$.
If $\alpha\equiv\beta \bmod \mu$ and $\gamma\equiv\delta \bmod \mu$, then $\alpha s\gamma\equiv\beta s\delta \bmod \mu$.
If $\alpha\equiv\beta \bmod \mu$ and $\gamma\equiv\delta \bmod \mu$, then $\alpha p\gamma\equiv\beta p\delta \bmod \mu$.

That these hold under our criterion $\alpha p\mu'=\beta p\mu'$ is evident.

Bell's statement of (1.5) has as its Boolean analogue:

$$\alpha \equiv \zeta \bmod \mu \text{ if and only if } \mu \text{ divides } \alpha.$$

Testing in interpretation I, we have that $\alpha\mu' = \omega$ if and only if $\mu | \alpha$; that is, $\alpha\mu' = \omega$ if and only if $\alpha\mu = \alpha$, which is true.

The Boolean analogue of Bell's (1.6) is the following:

If $\kappa\alpha \equiv \kappa\beta \bmod \mu$, then $\alpha \equiv \beta \bmod \kappa r\mu$.

Under interpretation I, the hypothesis is $(\kappa\alpha)\mu' = (\kappa\beta)\mu'$, and the conclusion $\alpha(\mu + \kappa')' = \beta(\mu + \kappa')'$; but these statements are identical.

Bell's last condition (1.7) is intended to furnish the analogue of the following in rational arithmetic: $a \equiv a \bmod m$. Such an analogue holds, under Bell's (4.1, 4.2), *only* in the special form (equivalent in the rational case) $0 \equiv 0 \bmod m$. But obviously with the definition of the present paper, we have the *complete* analogue

$$\alpha \equiv \alpha \bmod \mu.$$

In close relationship to this result lies the fact that under Bell's form of congruence no two elements of a Boolean algebra can be congruent unless each is congruent to the arithmetic zero. Indeed, we may compare the generality of the two ideas by observing that while our definition makes $\alpha \equiv \beta \bmod \mu$ if and only if $\alpha p\mu' = \beta p\mu'$, Bell's definition makes $\alpha \equiv \beta \bmod \mu$ if and only if $\alpha p\mu' = \beta p\mu' = \zeta$; the latter thus singles out *one* of the residue classes into which we shall in the next section distribute all the elements of a Boolean algebra.

5. **Residue classes.** In rational number theory (with positive and negative integers) a and b belong to the same residue class with respect to m if $a \equiv b \bmod m$. The residue class of an element a contains all elements x which can be written in the form $x = a + my$. If we restrict ourselves to non-negative integers we may say that the residue class of a consists of all x such that $x = a + my$ and all x such that $a = x + my$. We may then naturally call an element a of a residue class the generator of the class if every member x of the class can be written in the form $x = a + my$. We shall say similarly for $\mathfrak{B}$: the *residue class* of α consists of all ξ such that $\xi = \alpha s(\mu p\eta)$ and all ξ such that $\alpha = \xi s(\mu p\eta)$; α is the *generator* of its residue class if and only if every member ξ of the class can be written in the form $\xi = \alpha s(\mu p\eta)$. The following theorems are then analogues of theorems in the non-negative rational case:

Every residue class with respect to a modulus μ possesses one and only one generator.

$\alpha \equiv \beta \bmod \mu$ *if and only if α and β belong to the same residue class with respect to the modulus μ.*

We shall confine the proofs to interpretation I. To prove the first theorem, let α be any member of a residue class; then $\alpha_0=\alpha\mu'$ is a generator. For if either $\xi=\alpha+\mu\eta$ or $\alpha=\xi+\mu\eta$, then $\xi\mu'=\alpha\mu'$, and $\xi=\alpha_0+\mu\xi$. There can not be two distinct generators α_0, α_1; for if $\alpha_1=\alpha_0+\mu\eta_0$ and $\alpha_0=\alpha_1+\mu\eta_1$, it follows that $\alpha_1|\alpha_0$ and $\alpha_0|\alpha_1$, so that $\alpha_1=\alpha_0$.

The second theorem is obvious, since the generators of the residue classes of α and β, which are respectively $\alpha\mu'$ and $\beta\mu'$, will be equal if and only if $\alpha\equiv\beta \bmod \mu$.

It is clear that the elements of a Boolean algebra which can participate in Bell's definition of congruence are those belonging to the single residue class whose generator is ζ.

6. Coprimality. Two elements α, β of a Boolean algebra are called *coprime* (Bell, (22.1)) when $\alpha g\beta=\upsilon$. We may express this in terms of congruence (without any precise analogue in rational arithmetic): *α and β are coprime if and only if $\alpha\equiv\upsilon \bmod \beta$.* For the definition of coprimality, $\alpha g\beta=\upsilon$, is the same as $\alpha s\beta=\upsilon$, which is equivalent to $\alpha p\beta'=\upsilon p\beta'$ or $\alpha\equiv\upsilon \bmod \beta$.

7. The linear congruence; arithmetic reciprocals. It is remarkable that while algebraic division (i.e., solution of linear equation) in $\mathfrak{L}$ is nearly always impossible or non-unique, arithmetic division with respect to a modulus is unique under the same hypotheses as in rational arithmetic and possible under the same hypotheses as in rational arithmetic.

If α, μ are coprime, there exists one and (congruentially) only one ξ such that $\alpha p\xi\equiv\beta \bmod \mu$.

For $\alpha\equiv\upsilon \bmod \mu$, by the preceding section, and $\xi\equiv\xi \bmod \mu$; thus the given congruence is equivalent to $\xi\equiv\beta \bmod \mu$.

As a special case we have the following:

If α, μ are coprime, then α has with respect to the modulus μ one and (congruentially) only one reciprocal.

The value of the reciprocal is given by $\xi\equiv\alpha\equiv\upsilon \bmod \mu$.

For the case of more general α, μ we have the following theorem:

The congruence $\alpha p\xi\equiv\beta \bmod \mu$ has no solution unless $(\alpha g\mu)\beta d$; if this condition holds, and

$$\alpha g\mu = \delta, \qquad \delta r\mu = \mu_1, \qquad \alpha = \delta p\alpha_1, \qquad \beta = \delta p\beta_1,$$

then every solution is given by

$$\xi \equiv \xi_1 s(\eta p\mu_1) \bmod \mu,$$

where ξ_1 *is a properly selected element of the algebra satisfying the congruence* $\alpha_1 p\xi_1 \equiv \beta_1 \bmod \mu_1$, *and* η *is arbitrary.*

We give the proof under interpretation I. Let

$$\alpha\xi \equiv \beta \bmod \mu, \tag{1}$$

$$\delta = \alpha + \mu. \tag{2}$$

Then

$$\alpha\xi\mu' = \beta\mu', \qquad \beta = \alpha\xi\mu' + \beta\mu ;$$

since $\delta \,|\, \alpha$ and $\delta \,|\, \mu$, it follows that $\delta \,|\, \beta$.

Now let

$$\mu_1 = \delta' + \mu, \qquad \alpha = \delta\alpha_1, \qquad \beta = \delta\beta_1. \tag{3}$$

The congruence $\alpha_1\xi_1 \equiv \beta_1 \bmod \mu_1$ has a solution; for

$$\begin{aligned} \alpha_1 + \mu_1 &= \alpha_1(\delta + \delta') + (\delta' + \mu) = (\alpha_1\delta + \mu) + (\alpha_1\delta' + \delta') \\ &= (\alpha + \mu) + \delta' = \delta + \delta' = \epsilon, \end{aligned}$$

so that α_1, μ_1 are coprime and $\alpha_1 \equiv \epsilon \bmod \mu_1$. A solution is $\xi_1 = \beta$; for $\alpha_1\xi_1 = \alpha_1\beta = \alpha_1\delta\beta_1 \equiv \epsilon\delta\beta_1 \equiv \delta\beta_1 \equiv \beta \bmod \mu_1$. We shall show that

$$\xi \equiv \beta + \eta\mu_1 \bmod \mu \tag{4}$$

is for every η a solution of (1). By (2), (3), $\alpha \equiv \delta \bmod \mu$, and $\mu_1 \equiv \delta' \bmod \mu$; hence

$$\begin{aligned} \alpha\xi &\equiv \delta\xi \equiv \delta\beta + \eta\delta\mu_1 \bmod \mu, \\ \alpha\xi &\equiv \beta + \eta\delta\delta' \bmod \mu, \\ \alpha\xi &\equiv \beta \bmod \mu. \end{aligned}$$

Conversely every solution of (1) is of the form (4) for some η. For from (1) and (3) we deduce that $\delta\alpha_1\xi \equiv \delta\beta_1 \bmod \mu$, and by Bell, (1.5),

$$\alpha_1\xi \equiv \beta_1 \bmod \mu_1.$$

Hence $\xi \equiv \beta_1 \bmod \mu_1$, ξ is with respect to μ_1 in the residue class generated by $\beta_1\mu_1'$, and $\xi = \beta_1\mu_1' + \eta\mu_1$. But $\beta_1\mu_1' = \beta_1\delta\mu' = \beta\mu'$, $\beta_1\mu_1'$ is with respect to μ in the residue class generated by $\beta\mu'$, and $\beta_1\mu_1' \equiv \beta \bmod \mu$. Thus (4) must hold.

Cornell University,
Ithaca, N. Y.