## ALGORITHM 99

EVALUATION OF JACOBI SYMBOL STEPHEN J. GARLAND AND ANTHONY W. KNAPP Dartmouth College, Hanover, N. H.

procedure Jacobi (n, m, r); value n, m;

integer n, m, r;

**comment** Jacobi computes the value of the Jacobi symbol (n/m), where *m* is odd, by the law of quadratic reciprocity. The parameter *r* is assigned one of the values -1, 0, or 1 if *m* is odd. If *m* is even, the symbol is undefined and *r* is assigned the value 2. For odd *m*, the routine provides a test of whether *m* and *n* are relatively prime. The value of *r* is 0 if and only if *m* and *n* have a nontrivial common factor. In the special case where *m* is prime, r = -1 if and only if *n* is a quadratic nonresidue of *m*;

## begin

```
integer s;
   Boolean p, q;
   Boolean procedure parity (x); value x; integer x;
      comment The value of the parity function is true if x is
         odd, false if x is even;
      begin
         parity := x \div 2 \times 2 \neq x
      end parity;
   if \neg parity (m) then begin r := 2; go to exit end;
   p := true;
   loop: n := n - n \div m \times m;
          q := false;
          if n \leq 1 then go to done;
   even: if \neg parity (n) then
          begin
            q := \neg q;
            n := n \div 2;
            go to even
          end n now odd;
          if q then if parity ((m\uparrow 2 - 1) \div 8) then p := \neg p;
          if n = 1 then go to done;
          if parity ((m-1) \times (n-1) \div 4) then p := \neg p;
          s := m; m := n; n := s; go to loop;
   done: r := if n = 0 then 0 else if p then 1 else -1;
        end Jacobi
exit:
```

© ACM, 1962. This is the author's version of the work. It is posted here by permission of ACM for your personal use. Not for redistribution. The definitive version was published in *Communications of the ACM* 5:6, pages 345–346, June 1962 (http://dl.acm.org/citation.cfm?doid=367766.368172).