```
┌──────────────────────────── MODULE ecc ────────────────────────────┐
EXTENDS Integers, Sequences, TLC

p ≜ 203
a ≜ 5
b ≜ 13
Gx ≜ 4
Gy ≜ 5
n ≜ 19
G ≜ ⟨Gx, Gy⟩

VARIABLES x, y, scalar, P, Q, R, k, s, d, r, z, validPoint

EllipticCurve(e, f) ≜
    (f^2) = (e^3 + a ∗ e + b)%p

ValidPoint(f, e) ≜
    EllipticCurve(f, e)

InverseMod(m, l) ≜
    LET
        RECURSIVE extendedGCD(_, _)
        extendedGCD(u, v) ≜ IF v = 0 THEN ⟨u, 1, 0⟩
                                   ELSE
                                      LET res ≜ extendedGCD(v, u%v)IN
                                      ⟨res[1], res[3], res[2] − (u ÷ v) ∗ res[3]⟩
        gcdRes ≜ extendedGCD(m, l)
        gcd ≜ gcdRes[1]
        inv ≜ gcdRes[2]%p
    IN  IF gcd = 1 THEN inv ELSE 0

PointAddition(J, K) ≜
    LET
        x1 ≜ J[1]
        y1 ≜ J[2]
        x2 ≜ K[1]
        y2 ≜ K[2]
        slope ≜ IF (x1 = x2) THEN (((3 ∗ x1^2   + a) ∗ InverseMod(2 ∗ y1, p))%p)
                ELSE  (y2 − y1) ∗ InverseMod(x2 − x1, p)%p
    IN
        ∧ x′ = (slope^2 − x1 − x2)%p
        ∧ y′ = ((slope ∗ (x1 − x′)) − y1)%p
        ∧ R′ = ⟨x′, y′⟩

RECURSIVE Bits(_)
Bits(scal) ≜
     IF scal = 0 THEN ⟨⟩
```

```
      ELSE  Append(Bits(scal ÷ 2), scal%2)

ScalarMultiplication(scal, J) ≜
    LET
        bits ≜ Bits(scal)
        R_init ≜ ⟨0, 0⟩
        Q_init ≜ J
        result  ≜ [R_acc ∈ 1 . . Len(bits) ↦
                      IF bits[R_acc] = 1
                       THEN PointAddition(R_init, Q_init)
                       ELSE  R_init]
        final_R ≜ result[Len(bits)]
    IN  final_R

GeneratePublicKey(d_) ≜
    ScalarMultiplication(d_, G)

GenerateSignature(z_, d_) ≜
    LET
        kVal ≜ CHOOSE k_ ∈ 1 . . (n − 1) : TRUE
        Rval ≜ ScalarMultiplication(kVal, G)
        rval  ≜ IF Rval[1] = 0 THEN 1 ELSE  Rval[1]%n
        sval  ≜ ((z_ + rval ∗ d_) ∗ InverseMod(kVal, n))%n
    IN
        ⟨rval, sval⟩

ValidateSignature(r_, s_, z_, Q_) ≜
    LET
        w ≜ InverseMod(s_, n)
        u1 ≜ (z_ ∗ w)%n
        u2 ≜ (r_ ∗ w)%n
        X ≜ PointAddition(ScalarMultiplication(u1, G), ScalarMultiplication(u2, Q_))
    IN
        ∧ r_ = X[1]%n
        ∧ r_ ≠ 0
        ∧ s_ ≠ 0

Init ≜
    ∧ x  = Gx
    ∧ y  = Gy
    ∧ k  = 3
    ∧ s  = 5
    ∧ d  = 7
    ∧ r  = 11
    ∧ z  = 13
    ∧ P = G
```

$\quad \land\ Q = \langle Gx,\ Gy \rangle$
$\quad \land\ R = \langle 0,\ 0 \rangle$
$\quad \land\ validPoint = ValidPoint(Gx,\ Gy)$
$\quad \land\ scalar = 17$

$Next\ \triangleq$
$\quad \lor\ \exists\, M \in \{\langle x,\ y \rangle\} : ValidPoint(x,\ y) \land P' = M$

$Spec\ \triangleq$
$\quad Init \land \Box[Next]_{\langle x,\, y,\, scalar,\, P,\, Q,\, R,\, k,\, s,\, d,\, r,\, z,\, validPoint \rangle}$