```
──────────────────────────── MODULE ecc ────────────────────────────
EXTENDS Integers, Sequences, TLC, Bitwise

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]%l
    IN
        IF gcd ≠ 1 THEN
            IF gcd = 0 THEN 0 ELSE ⟨0, "Error: gcd(m, l) is not 1"⟩
         ELSE
            IF inv < 0 THEN inv + l ELSE inv


PointAddition(J, K) ≜
    LET
        x1 ≜ J[1]
        y1 ≜ J[2]
        x2 ≜ K[1]
        y2 ≜ K[2]
        isNeutral(A) ≜ (A = ⟨0, 0⟩)
        slope ≜
            IF isNeutral(J) THEN
                ⟨x2, y2⟩
             ELSE IF isNeutral(K) THEN
            $\langle x1,\ y1 \rangle$
          ELSE  IF $(x1 = x2) \land (y1 = y2)$ THEN
            $((3 * x1^2 + a) * InverseMod(2 * y1,\ p))\%p$
          ELSE  IF $(x1 = x2) \land (y1 \neq y2)$ THEN
            $\langle 0,\ 0 \rangle$
          ELSE
            $((y2 - y1) * InverseMod(x2 - x1,\ p))\%p$
    IN
       IF $(x1 = x2) \land (y1 \neq y2)$ THEN
          $\land\ x' = 0$
          $\land\ y' = 0$
          $\land\ R' = \langle x',\ y' \rangle$
        ELSE
          $\land\ x' = (slope^2 - x1 - x2)\%p$
          $\land\ y' = ((slope * (x1 - x')) - y1)\%p$
          $\land\ R' = \langle x',\ y' \rangle$


RECURSIVE $Bits(\_)$
$Bits(scal) \triangleq$
     IF $scal = 0$ THEN $\langle\rangle$
      ELSE  $Append(Bits(scal \div 2),\ scal\%2)$

$ScalarMultiplication(scal,\ J) \triangleq$
    LET
        $bits \triangleq Bits(scal)$
        $R\_init \triangleq \langle 0,\ 0 \rangle$
        $Q\_init \triangleq J$
        $result \triangleq [R\_acc \in 1\ ..\ Len(bits) \mapsto$
                         IF $bits[R\_acc] = 1$
                          THEN $PointAddition(R\_init,\ Q\_init)$
                          ELSE  $R\_init]$
        $final\_R \triangleq result[Len(bits)]$
    IN  $final\_R$

$GeneratePublicKey(d\_) \triangleq$
    $ScalarMultiplication(d\_,\ G)$

$GenerateSignature(z\_,\ d\_) \triangleq$
    LET
        $SecureRandomSet \triangleq \{k\_ \in 1\ ..\ (n - 1) : \text{TRUE}\}$
        $kVal \triangleq$ CHOOSE $k\_ \in SecureRandomSet : \text{TRUE}$
        $Rval \triangleq ScalarMultiplication(kVal,\ G)$
        $rval \triangleq$ IF $Rval[1] = 0$ THEN 1 ELSE  $Rval[1]\%n$
        $sval \triangleq ((z\_ + rval * d\_) * InverseMod(kVal,\ n))\%n$
    IN
```

```
        $\langle rval,\ sval \rangle$

$ValidateSignature(r\_,\ s\_,\ z\_,\ Q\_) \triangleq$
    LET
        $w \triangleq InverseMod(s\_,\ n)$
        $u1 \triangleq (z\_ * w)\%n$
        $u2 \triangleq (r\_ * w)\%n$
        $X \triangleq PointAddition(ScalarMultiplication(u1,\ G),\ ScalarMultiplication(u2,\ Q\_))$
    IN
        $\land\ r\_ = X[1]\%n$
        $\land\ r\_ \neq 0$
        $\land\ s\_ \neq 0$

$Init \triangleq$
    $\land\ x\ = Gx$
    $\land\ y\ = Gy$
    $\land\ k\ = 3$
    $\land\ s\ = 5$
    $\land\ d\ = 7$
    $\land\ r\ = 11$
    $\land\ z\ = 13$
    $\land\ P = G$
    $\land\ Q = \langle Gx,\ Gy \rangle$
    $\land\ R = \langle 0,\ 0 \rangle$
    $\land\ validPoint = ValidPoint(Gx,\ Gy)$
    $\land\ scalar = 17$

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

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