Standard curve database

CROCS
Centre for Research on Cryptography and Security

GitHub

P-256

256-bit prime field Weierstrass curve.
Also known as: secp256r1 prime256v1

$$y^2 \equiv x^3 + ax + b$$

Parameters

Name	Value
p	0xffffffff00000001000000000000000000000000ffffffffffffffffffffffff
a	0xffffffff00000001000000000000000000000000fffffffffffffffffffffffc
b	0x5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d26
G	(0x6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898 0x4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf5
n	0xffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632
h	0x1

Characteristics

- **OID**: 1.2.840.10045.3.1.7
- **Seed**: C49D360886E704936A6678E1139D26B7819F7E90
- **j-invariant**: 7958909377132088453074743217357398615041065282494610304372115906626967530147
- **Trace of Frobenius**: 89188191154553853111372247798585809583
- **Discriminant**: 47064476442213300654454205837611899485069387829947879813735 60

1543372794627813

- **Anomalous**:
  false
- **Supersingular**:
  false
- **Embedding degree**:
  38597363070118749587565815649802524509998985074711920114140753020356170681456
- **CM-discriminant**:
  51463150760158332783421087533070032680028376163334078103224794776407756178469
- **Conductor**:
  3

SAGE

```
p = 0xffffffff00000001000000000000000000000000ffffffffffffffffffff
K = GF(p)
a = K(0xffffffff00000001000000000000000000000000fffffffffffffffffffc
b = K(0x5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e2
E = EllipticCurve(K, (a, b))
G = E(0x6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945
E.set_order(0xffffffff00000000ffffffffffffffffbce6faada7179e84f3
```

SAGE SAGE

PARI/GP

```
p = 0xffffffff00000001000000000000000000000000ffffffffffffffffffff
a = Mod(0xffffffff00000001000000000000000000000000fffffffffffffffffffc
b = Mod(0x5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c2
E = ellinit([a, b])
E[16][1] = 0xffffffff00000000ffffffffffffffffbce6faada7179e84f3b
G = [Mod(0x6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a139
```

PARI/GP PARI/GP

JSON


```
{
  "name": "P-256",
  "desc": "",
  "oid": "1.2.840.10045.3.1.7",
  "form": "Weierstrass",
  "field": {
    "type": "Prime",
    "p": "0xffffffff00000001000000000000000000000000ffffffffffff
    "bits": 256
  },
  "params": {
    "a": {
      "raw": "0xffffffff00000001000000000000000000000000fffffffc
    },
    "b": {
      "raw": "0x5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f6
    }
  },
  "generator": {
    "x": {
      "raw": "0x6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0
    },
    "y": {
      "raw": "0x4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ece
    }
  },
  "order": "0xffffffff00000000ffffffffffffffffbce6faada7179e84f3
  "cofactor": "0x1",
  "aliases": [
    "secg/secp256r1",
    "x962/prime256v1"
```

```
  ],
  "characteristics": {
    "seed": "C49D360886E704936A6678E1139D26B7819F7E90",
    "j_invariant": "7958909377132088453074743217357398615041065
    "anomalous": false,
    "cm_disc": "5146315076015833278342108753307003268002837616
    "conductor": "3",
    "discriminant": "4706447644221330065445420583761189948506938
    "embedding_degree": "385973630701187495875658156498025245099
    "torsion_degrees": [
      {
        "full": 3,
        "least": 3,
        "r": 2
      },
      {
        "full": 6,
        "least": 2,
        "r": 3
      },
      {
        "full": 10,
        "least": 2,
        "r": 5
      },
      {
        "full": 16,
        "least": 16,
        "r": 7
      }
    ],
    "supersingular": false,
    "trace_of_frobenius": "89188191154553853111372247798585809583
  }
}
```


JSON JSON