Práce se zabývá aritmetikou eliptických křivek nad konečnými tělesy a způsoby, jak tyto výpočty zefektivnit. V první části jsou pomocí pojmů a vět z algebraické geometrie definovány eliptické křivky a odvozeny jejich základní vlastnosti včetně základních algoritmů na počítání s body křivky. Ve druhé kapitole je vidět, jak lze výpočty zrychlit pomocí techniky time-memory tradeoff, tj. přidání redundance a konečně ve třetí zavádíme zcela nový tvar křivek, který je pro dané účely velmi efektivní.